UNIVERSITÉ DU QUÉBEC À MONTRÉAL

CYBERSÉCURITÉ ET GESTION DES RISQUES LIÉS À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS : CAS DES BANQUES CANADIENNES

MÉMOIRE

PRÉSENTÉ

COMME EXIGENCE PARTIELLE

DE LA MAÎTRISE EN COMPTABILITÉ, CONTRÔLE, AUDIT

PAR
ANANI BADJAGBO

Janvier 2025

UNIVERSITÉ DU QUÉBEC À MONTRÉAL
Service des bibliothèques

Avertissement

REMERCIEMENTS

Je tiens à remercier toutes les personnes qui m'ont soutenu tout au long de ce projet qui s'est amorcé il y a maintenant plus de deux ans. Mes remerciements vont d'abord à Mme Rachel Papirakis, ma directrice de recherche, pour avoir accepté de m'encadrer. Je la remercie pour sa disponibilité, son savoir et sa volonté de m'inculquer ses connaissances ainsi qu'en raison de son appui et de ses critiques essentielles pour ma croissance. De plus, je lui suis reconnaissant pour ses précieux conseils et son engagement pour mener à bien ce projet de recherche. Mes remerciements auxprofesseurs dont les cours excellents ont contribué à élargir mes horizons et pour leurs nourrissants conseils : Mme Camélia Radu, directrice de programme, Mme Paulina Arroyo Pardo, M. Toudert Abdelmadjid, Mme Dicko Saidatou, Mme Madalina Solcanu, M. Richard Fontaine, M. Marc Chabot, Mme Khemakhem Hanen, Mme Fakhfakh Saoussen et M. Robert Robillard.

DÉDICACE

Je dédie ce mémoire à mes défunts parents qui ont toujours souhaités ma réussite, à ma femme Vanessa, à mes frères, spécialement à Dr Koffi et sa femme Reine Jacqueline, à Past. Dominique, à mes belles sœurs, à mes ami(e)s et à notre fille Adorée pour leurs soutiens et encouragements, aux directeurs : Mme Lucie Bassani, M. Ali, M. Ramanou Nassirou, M. Same Komla, M. Ange Kossivi Ketor, M. Dossa Komla et aux présidents : SEM Faure Essozimna Gnassingbé, SEM Guy Cormier et Marie-Huguette Cormier, SEM Martin Bilodeau et SEM Holman Rodriguez.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES ABRÉVIATIONS, DES SIGLES ET DES ACRONYMES

RGPD : Règlement général sur la protection des données

COSO: *Committee of Sponsoring Organizations of Treadway Commission* / Référentiel de contrôle interne

IFACI : Institut français d'audit et du contrôle internes

GRE : Gestion des Risques en Entreprise

OCDE : Organisme de Coopération et de Développement Économique

LPRPDE : Loi sur la protection des renseignements personnels et les documents électroniques

LPRPSP : Loi sur la protection des renseignements personnels dans le secteur privé

LCCJTI : Loi concernant le cadre juridique des technologies de l'information

LP : Loi sur le privé

LAI : Loi sur l'accès

PWC: *Pricewaterhouse Coopers*

SQL: *Structured Query Language*

URL : *Uniform Resource Locator*

EFVP : Évaluation des facteurs relatifs à la vie privé

SGSI : Les systèmes de gestion de la sécurité de l'information

PCI DSS : Le Standard de Sécurité des Données de l'Industrie des Cartes de Paiement

BSIF : Bureau du surintendant des institutions financières

RÉSUMÉ

Cette recherche vise à illustrer l'importance de la cybersécurité et gestion des risques liés à la protection des renseignements personnels. De plus ce mémoire utilise des stratégies qui facilitent la compréhension des différents risques de protection des renseignements personnels, leur évaluation et la mise en œuvre de procédures appropriées pour y faire face. Ainsi, les institutions financières canadiennes pourraient améliorer leurs missions d'audit interne en matière de protection des renseignements personnels en utilisant les résultats de la recherche pour contrôler les risques plus efficacement.

Dans notre recherche, nous avons appliqué le cadre conceptuel des risques, qui est un processus qui vise à identifier, évaluer et gérer les risques qui pourraient affecter la réalisation des objectifs d'une organisation, et la théorie de la signalisation, qui souligne la divulgation proactive de données pertinentes ou la communication proactive d'informations. Nous nous sommes référés aux recherches scientifiques, de la législation de loi sur la protection des renseignements personnels, aux études réalisées par les grands cabinets de protection des renseignements personnels au Canada et à l'international et aux études de recherches menées par le Commissariat à la protection de vie privée du Canada. Dans nos travaux pratiques, nous avons examiné les procédures liées à la gestion des risques de protection des données personnelles par l'analyse des rapports annuels sur trois années de trente-quatre banques canadiennes sélectionnées des plus de soixante banques exerçant leurs activités au Canada. Cela nous a permis d'identifier les risques de protection des renseignements personnels, ainsi que les mesures de gestion des risques mises en place à cet égard. Les résultats de cette étude révèlent que, si certaines institutions, telles que les banques canadiennes, mettent en place des stratégies claires pour gérer les risques liés à la protection des renseignements personnels et aux cybermenaces, le manque de processus adéquats peut engendrer des difficultés qui affectent l'ensemble des activités de l'entreprise. Également, cette recherche contribue au développement d'un modèle de gestion des risques de protection des renseignements personnels et encourage le conseil d'administration et la haute direction des institutions financières canadiennes à inclure la protection des renseignements personnels dans leur charte d'audit interne.

Mots clés: Cybersécurité, gestion de risques, protection des renseignements personnels

ABSTRACT

This research aims to illustrate the importance of cybersecurity and risk management related to the protection of personal information. Furthermore, this paper utilizes strategies that facilitate the understanding of various risks to personal information, their assessment, and the implementation of appropriate procedures to address them. Thus, Canadian financial institutions could improve their internal audit missions concerning personal information protection by using the research findings to manage risks more effectively.

In our research, we applied the conceptual framework of risks, which is a process aimed at identifying, assessing, and managing risks that could affect the achievement of an organization's objectives, and signaling theory, which emphasizes the proactive disclosure of relevant data or proactive communication of information. We referred to scientific research, legislation on personal information protection, studies conducted by major personal information protection firms in Canada and internationally, and research studies conducted by the Office of the Privacy Commissioner of Canada. In our practical work, we examined the procedures related to personal data risk management by analyzing the annual reports over three years from thirty-four selected Canadian banks out of more than sixty banks operating in Canada. This allowed us to identify the risks of personal information protection as well as the risk management measures implemented in this regard. The results of this study reveal that, while some institutions, such as Canadian banks, have clear strategies in place to manage risks related to the protection of personal information and cyber threats, the lack of adequate processes can create difficulties that affect all of the company's activities. Additionally, this research contributes to the development of a personal information protection risk management model and encourages the board of directors and senior management of Canadian financial institutions to include personal information protection in their internal audit charter.

Keywords: Cybersecurity, risks management, personals informations protection

INTRODUCTION

Notre recherche vise à comprendre comment les banques canadiennes divulguent les risques reliés à la protection des renseignements personnels et les stratégies défensives qu'elles mettent en place pour gérer ces risques. L'avènement de l'ère numérique a provoqué une transformation profonde du paysage financier, offrant aux consommateurs des services bancaires en ligne à la fois pratiques et efficaces. Le numérique a révolutionné la façon dont ces institutions fonctionnent et interagissent avec les consommateurs et les citoyens (Le Maux, 2019). Toutefois, cette entrée rapide dans le monde immatériel comporte des risques. Cette transition vers la virtualisation des transactions financières a engendré de nouveaux défis en termes de cybersécurité et de préservation des renseignements personnels.

En effet, les systèmes informatiques, les réseaux et autres appareils électroniques des organisations sont susceptibles de subir diverses attaques cybernétiques (Mongin, 2013). Les cyberattaques peuvent prendre de nombreuses formes, notamment des virus, des logiciels malveillants, des ransomwares, des attaques par déni de service et bien d'autres. Toutes les formes d'attaques visant des réseaux informatiques ou des systèmes d'information sont communément appelées cybercriminalité (Lagare, 2021). La cybercriminalité constitue pour le secteur financier une menace qui suscite actuellement une attention accrue de la part des organismes de surveillance du monde entier (Fernandez-Bollo, 2015).

Les observations de la dernière décennie sur la cybercriminalité et les abus du numérique ont montré que les activités illégales visant à obtenir de l'argent ou des informations ne se limitent plus aux confins du cybermonde. À l'heure où l'Internet des objets devient un domaine d'activité humaine, ce type de risque doit être pris en compte, d'autant plus qu'il est difficile d'en évaluer les conséquences en raison de l'ampleur du changement (Freyssinet, 2013).

La cybersécurité s'est érigée en enjeu majeur pour l'ensemble du secteur bancaire, et les institutions financières au Canada ne font pas exception à cette règle. Desjardins, une des plus grandes coopératives financières au Canada, a été victime d'une cyberattaque en juin 2019. Près de 8 millions de personnes ont été touchées avec leurs informations personnelles, ainsi que leurs

numéros d'assurance sociale et leurs coordonnées bancaires. Selon Desjardins, cette situation a causé à l'entreprise des coûts de 108 millions de dollars, y compris des frais juridiques, des services de surveillance et une provision pour la protection contre le vol d'identité (Gril, 2021).

BMO et Simplii Financial de CIBC ont été simultanément victimes d'une cyberattaque en mai 2018. Plusieurs milliers de clients ont été touchés et des informations personnelles telles que les numéros de compte bancaire, les adresses, le numéro d'assurance sociale et la date de naissance ont été compromises. Par la suite, les pirates ont essayé d'obtenir de l'argent des clients en échange de promesses de non-divulgation de leurs données personnelles. Ce vol de données personnelles a touché plus de 10 000 clients de l'unité Simplii Financial de CIBC et plus de 113 000 clients de la BMO. Les pertes financières s'élèvent à 21,2 M$ pour BMO et à 1,8 M$ pour CIBC (Pomerleau & Lowery, 2020).

Aux États-Unis, la banque *JPMorgan Chase* a subi une cyberattaque en septembre 2014. Plus de 83 millions de clients et 7 millions d'entreprises ont subi des vols d'informations personnelles. Cette attaque est considérée comme l'une des violations de données les plus graves de l'histoire des États-Unis (Lemieux, 2015).

Face à la prolifération et à l'ampleur des cyberattaques visant à compromettre les données sensibles des clients et à perturber le fonctionnement quotidien des banques, la gestion des risques liés aux renseignements personnels est devenue une priorité absolue pour les institutions financières. Les employeurs, les salariés, les représentants du personnel, les chargés de prévention et les organismes institutionnels accordent une grande attention à l'émergence de ce nouveau risque.

À cet effet, la mise en place de mesures pour une meilleure gestion des risques liés à la sécurité des informations personnelles permettra de réduire de nombreux risques, dont le risque de litige en matière de sécurité des renseignements personnels auquel pourraient être confrontées les institutions financières canadiennes en cas de non-respect des réglementations en matière de protection des données personnelles, tel que le Règlement général sur la protection des données (RGPD). Les procédures doivent être conformes aux exigences des lois canadiennes sur la protection de la vie privée. Les banques doivent ainsi déployer des mesures de protection

rigoureuses afin de prévenir les brèches de données et de maintenir la confiance de leur clientèle dans un contexte de menace constante. Ces mesures visent à donner plus de crédibilité aux institutions auprès de leurs parties prenantes[1].

L'objectif de cette étude sur la cybersécurité et la gestion des risques liés à la protection des renseignements personnels dans le cas des banques canadiennes est de comprendre comment les banques canadiennes divulguent les risques reliés à la protection des renseignements personnels et les stratégies défensives qu'elles mettent en place pour gérer ces risques. Plus spécifiquement, cette recherche vise à vérifier si les banques canadiennes inventorient et divulguent les risques liés à la protection des renseignements personnels dans leurs opérations, à recenser les risques liés à la confidentialité des renseignements personnels divulgués par les banques, et à relever les mesures de sécurité mises en place pour protéger les données personnelles des clients. Ce travail contribuera à améliorer les politiques et les pratiques de gestion des risques dans le secteur bancaire canadien, permettant ainsi de garantir la confidentialité et l'intégrité des données des clients et de renforcer la confiance du public dans le système financier du pays.

La législation en matière de cybersécurité

La Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, précédemment connue sous le nom de projet de loi no 64, apporte des modifications significatives aux lois sur la protection des renseignements personnels, dans le cadre de la juridiction provinciale du Québec (Rico, 2020). En vigueur depuis le 22 septembre 2021, cette loi vise à accorder plus de contrôle aux citoyens sur leurs renseignements personnels et à accroître la responsabilité des organisations en ce qui concerne leur gestion de ces renseignements. Elle actualise le cadre législatif pour le mettre en adéquation avec la réalité technologique actuelle. La protection des données personnelles est une préoccupation majeure dans une société de plus en plus tournée vers l'intelligence artificielle (IA). Les algorithmes d'IA sont de plus en plus exploités

[1] https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/ consulté : 2024-04-28 à14 :22 :10

pour collecter, analyser et exploiter des données personnelles, ce qui peut conduire à des atteintes à la vie privée et à un manque de confiance dans les systèmes technologiques (Silvestre Pinheiro, 2022). Par conséquent, il est essentiel d'établir des réglementations et des politiques de protection des données pour garantir que les informations personnelles sont collectées et utilisées de manière responsable (Akkour, Haounani, et al., 2023). Si le respect du Règlement général sur la protection des données (RGPD) entraîne inévitablement de nouvelles obligations pour les entreprises, il constitue également pour elles l'opportunité de renforcer la transparence concernant leurs politiques de protection des données personnelles. Ceci, à son tour, contribue à inspirer confiance aux citoyens quant à la gestion de leur données (Gola, 2017). Le respect du Règlement général sur la protection des données (RGPD) implique de se conformer aux règles et aux principes énoncés dans ce règlement de l'Union européenne. Cela signifie notamment de garantir la confidentialité, la sécurité et le traitement légal des données personnelles des citoyens européens. Les organisations qui collectent, traitent ou stockent des données personnelles doivent respecter les droits des individus sur leurs propres données, comme le droit à l'information, le droit d'accès, le droit de rectification, le droit à l'effacement, le droit à la limitation du traitement, le droit à la portabilité des données et le droit d'opposition. Il est essentiel de mettre en place des mesures appropriées pour assurer la conformité au RGPD, telles que la mise en œuvre de mesures de sécurité adéquates, la tenue de registres de traitement des données, la nomination d'un délégué à la protection des données si nécessaire, et la sensibilisation des employés aux bonnes pratiques de protection des donnée[2].

Le présent mémoire de recherche comporte cinq chapitres. Le premier résume les données de la littérature scientifique sur la gestion des risques sous trois angles : niveau général, international et canadien. Le deuxième chapitre expose le cadre théorique de la recherche. Le troisième chapitre présente la méthodologie utilisée. Elle se base sur l'étude de rapports annuels de trente-quatre

[2] https://www.deleguescommerciaux.gc.ca/tcs-sdc/guides/gdpr-eu-rgpd.aspx?lang=fra consulté : 2024-04-30 à 16 :08 :10

institutions financières canadiennes. Le quatrième chapitre est consacré à l'analyse des données recueillies. Le mémoire se termine par une conclusion et discussion des résultats.

CHAPITRE 1

REVUE DE LA LITTÉRATURE

Depuis l'émergence de la cybercriminalité, dans les années 1970, comme un défi majeur pour la sécurité numérique, les discussions récentes sur l'utilisation des données numériques et l'entrée en vigueur du nouveau règlement général européen sur la protection des données personnelles (RGPD) le 25 mai 2018 risquent de faire oublier que ces sujets s'inscrivent dans une continuité historique. En 1978, la création de la Commission nationale de l'informatique et des libertés (CNIL) en France a marqué une avancée significative. Les autorités publiques et les citoyens ont commencé à prendre en considération les enjeux émergents liés à l'informatique et à leurs implications sur les libertés individuelles[3]. L'évolution de la loi française en 1978 a commencé refléter la nécessité de lutter contre ces nouveaux types de délits liés à l'usage abusif de la technologie à la création de la Commission nationale de l'État (Holt et al., 2022). Dès 2001, la Loi sur la protection des renseignements personnels et des documents électroniques (LPRPDE), un texte de loi fédéral canadienne qui encadre le traitement des données personnelles par les entreprises privées, a été reconnue par la Commission Européenne comme garantissant un niveau de protection suffisant pour les données personnelles. La Loi 25 provinciale du Québec s'inspire fortement du Règlement général sur la protection des données (RGPD) européen et vise principalement à accorder davantage de droits aux individus qui partagent leurs informations personnelles, ainsi établit en même temps un principe général de transparence. Elle est le dernier développement législatif crucial dans le domaine de la protection de la vie privée au Canada, à la suite de l'approbation du projet de loi 64 en 2021, la Loi modernisant des dispositions législatives en matière de protection des renseignements personnels. Ce dernier a introduit des modifications significatives concernant la collecte, l'utilisation et la transmission des renseignements

[3] https://www.lhistoire.fr/1978-naissance-de-la-cnil consulté : 2024-04-28 à 15 :16 :03

personnels[4]. Une série d'études ont été publiées sur la cybersécurité, la gestion des risques liés à la protection des renseignements personnels, l'implication de l'audit interne dans l'évaluation de l'efficacité des mesures de protection des données personnelles et la législation. Le tour d'horizon de la revue de littérature vise à regrouper certaines des contributions les plus significatives, selon leurs objets, et à mettre en lumière la tendance actuelle dans le domaine de la sécurité de l'information et de la protection des données.

1.1 Cybercriminalité

On nomme cyberattaque une attaque qui cible des systèmes informatiques, des réseaux ou d'autres appareils électroniques (Mongin, 2013). Toutes les formes d'attaques visant des réseaux informatiques ou des systèmes d'information sont communément appelées cybercriminalité (Lagare, 2021). Les cyberattaques peuvent prendre diverses formes.

On peut trouver un excellent résumé des différents types de cyberattaques chez Cacciapaglia (2018) et Bendovschi (2015). Ils ont décrit jusqu'à neuf types d'attaques informatiques dans des rapports relativement récents :

- Le premier type de cyberattaque est connu sous le nom de *social engineering* qui est une attaque menée pour recueillir des informations sur des cibles potentielles ou les amener à effectuer des transactions ou des paiements. Elle exploite une faiblesse commune à tous les systèmes d'information existants, à savoir le facteur humain.
- Le second type de cyberattaque consiste en l'acquisition de mot de passes en ligne. Elle se produit lorsqu'un individu malveillant tente de deviner le mot de passe d'un utilisateur à l'aide de données spécifiques.
- Le troisième type de cyberattaque est le *phishing, spear-phishing et whaling*. C'est une pratique qui consiste à viser un "poisson", c'est-à-dire nous tous, lui envoyer un appât et

[4] (https://www.quebec.ca/nouvelles/actualites/details/loi-25-sur-la-protection-des-renseignements-personnels-des-citoyens-du-quebec-entree-en-vigueur-de-nouvelles-dispositions-qui-font-du-quebec-un-chef-de-file-mondial-50726, s. d.), consulté le 16/05/2024 à 07H 55

espérer qu'il morde à l'hameçon dans le but de récupérer des informations. C'est également une méthode utilisée pour obtenir illicitement des informations confidentielles des utilisateurs en se faisant passer pour une entité de confiance, telle qu'un site web réputé. Des milliers de personnes se font piéger chaque jour et révèlent leurs données personnelles et confidentielles (nom d'utilisateur, mot de passe et informations bancaires) à de mauvaises personnes ou se font infecter ou d'infecter son appareil.

- Le quatrième type de cyberattaque est la *SQL injection*. C'est une attaque qui exploite la syntaxe *SQL* et implique une injection requête *SQL* pour le code supplémentaire provoquant la manipulation des informations de la base de données. Le *SQL (Structured Query Language)* est un langage informatique qui permet d'utiliser des bases de données relationnelles, permettant de manipuler des données à travers de requêtes : lire, modifier, ajouter et supprimer ces dernières.
- Le cinquième type de cyberattaque est le *cross-site scripting (XSS)*. Il consiste à exploiter des vulnérabilités pour insérer du contenu malveillant, ce qui provoque alors des actions différentes de celles qui existent déjà sur la page. La vulnérabilité peut provenir de messages de forum ou de manipulation d'*URL (Uniform Resource Locator)*.
- Le sixième type de cyberattaque est le *malware*, vient du mot anglais *« malicious software »* qui signifie logiciels malveillants. Ils sont développés dans le but de causer des dommages ou de collecter des informations sur un système. Les logiciels malveillants, un terme global désignant les programmes nuisibles utilisés par les cybercriminels pour compromettre la confidentialité, la disponibilité et l'intégrité des données. Parmi les types de logiciels malveillants les plus répandus, on trouve les virus, les vers, les chevaux de Troie, les logiciels espions, les rançongiciels, les logiciels publicitaires et les logiciels effrayants.
- Le septième type de cyberattaque est la manipulation d'*URL*. Elle consiste à modifier les *URL* dans le navigateur de manière à accéder à des pages auxquelles l'on n'a pas accès.
- Le huitième type de cyberattaque porte le nom de *denial of service attack (DoS)*. Il consiste à rendre un service indisponible en lui envoyant un grand nombre de requêtes pour saturer un serveur. Vous devez savoir qu'un serveur a des capacités de communication limitées, donc si un acteur malveillant tente d'envoyer des requêtes répétées, le serveur peut commencer à ralentir et éventuellement rencontrer un problème. Une attaque par force brute

implique des essais répétés pour accéder à des données sécurisées (comme des mots de passe, des systèmes de cryptage, etc.) jusqu'à ce que la bonne clé soit découverte, permettant ainsi d'accéder aux informations protégées. La détection des attaques *DDoS* à la suite de foules flash est un problème difficile à résoudre. Les solutions existantes sont généralement destinées soit aux foules flash, soit aux attaques *DDoS,* et des recherches supplémentaires sont nécessaires pour avoir une approche globale permettant de répondre aux besoins de détection des variantes spoofées et non spoofées des attaques *DDoS* (Gera & Battula, 2018).

- Et enfin le neuvième type de cyberattaque est le *Man in the middle* ou l'homme au milieu qui est une attaque informatique visant à capter les communications entre deux parties sans qu'elles s'en rendent compte. L'attaque de l'homme du milieu survient lorsque l'attaquant s'insère entre les deux parties qui communiquent, ce qui lui permet d'intercepter chaque message envoyé de la source A à la source B avant qu'il n'atteigne sa destination prévue. Les dangers de ce type d'attaque incluent la possibilité d'accéder à des informations confidentielles de manière non autorisée et la capacité de modifier les données ou messages en transit entre l'émetteur et le destinataire (Bendovschi, 2015) et Cacciapaglia, 2018).

Les menaces en ligne augmentent. Le Club des experts de la sécurité de l'information et du numérique (CESIN) a partagé les conclusions de son enquête en janvier 2024 sur la cybersécurité des entreprises françaises, menée par *OpinionWay* pour le CESIN dans sa 9ème édition du baromètre annuel. Parmi les 456 répondants, 49% ont déclaré avoir subi au moins une cyberattaque, avec le *Phishing* signalé par 60% comme principale méthode d'attaque. Les attaques en déni de service sont en augmentation, touchant 39% des entreprises. De plus, 65% des entreprises ont subi des perturbations dans leur production à la suite d'attaques. Malgré ces défis, 87% des répondants ont une confiance élevée dans les solutions de sécurité, et la moitié des entreprises adoptent des offres de *startups*. Environ 1/3 à 1/4 des entreprises ont une part importante de leur système d'information dans le *Cloud*. En outre, 70% des entreprises ont été séduites par la Cyberassurance, et 70% sont actuellement impactées par une réglementation liée à la cybersécurité ou à l'Intelligence Artificielle (IA). En interne, 46% des Responsables Sécurité des Systèmes

d'Information (RSSI) ont observé l'utilisation de l'IA[5]. Le coût de la criminalité numérique à l'échelle mondiale ne cesse d'augmenter et dépasse les 3 000 milliards de dollars selon les données de 2015. Les entreprises cotées en bourse aux États-Unis signalent les risques commerciaux dans leurs rapports financiers déposés auprès de la *Securities and Exchange Commission* (SEC) en se basant sur les directives fournies en matière de déclaration des cyber-risques. De plus, des attaques informatiques notables ont visé récemment des entreprises renommées comme Sony, Target, *Home Depot*, Yahoo (Fisher et al., 2019). Fisher et al. (2019) dans leur recherche en cybercriminalité, ont utilisé le système *Wharton Research Data Services* pour examiner les rapports de la SEC. Une analyse chronologique a été menée sur les sociétés cotées en bourse aux États-Unis ayant évoqué la cybercriminalité comme un risque de 2002 à 2018. Il est apparu que 2,8 % des entreprises ont identifié le risque cybernétique comme une préoccupation majeure dans leurs rapports financiers (formulaire 10-K) pour l'année 2017. Ce document traite de façon détaillée du faible niveau de déclaration des risques liés au cyberespace, examine les raisons pour lesquelles les entreprises effectuent ces déclarations et identifie les obstacles qui limitent leur augmentation (incluant la couverture d'assurance cyber, la rétroaction négative, la dépréciation des actions, la responsabilité juridique potentielle et des éléments dissuasifs à la déclaration). En conclusion, il est recommandé que la SEC mobilise les parties prenantes (telles que les entreprises, les investisseurs, les organismes de réglementation et le département de la Sécurité intérieure des États-Unis) pour concevoir un cadre de gestion des risques cybernétiques qui garantisse une cohérence accrue dans la déclaration de ces risques.

Lorsque des attaques de cybercriminalité affectent les institutions financières, nous pouvons observer des réactions plus virulentes (Iat, 2020). En effet, d'une part, les institutions financières traitent de grandes quantités d'informations sensibles des clients, incluant des informations personnelles telles que leur situation financière, leur historique de crédit et leurs antécédents en matière de conduite. Ces informations hautement confidentielles peuvent être utilisées pour effectuer des transactions frauduleuses ou d'autres actes nuisibles si elles tombent entre de mauvaises mains (Kablan et al., 2023). D'autre part, les lois financières sont complexes. En matière

[5] https://systematic-paris-region.org/barometre-annuel-du-cesin/ consulté : 2024-04-29 à 14 :27 :13

de protection des renseignements personnels, les institutions financières sont soumises à des réglementations strictes et difficiles à comprendre (De Coussergues et al., 2020). Les annonces publiques de cyberattaques dans ce secteur diminuent considérablement la confiance des clients et des investisseurs car elles sont généralement associées aux vols de données personnelles. Les entreprises sont quotidiennement touchées par des cyberattaques. « Il existe deux types d'entreprises : celles qui ont été piratées et celles qui ne le savent pas encore », a déclaré John Chambers, ancien PDG de Cisco. Dans *l'Annual CybersecurityReport* de Cisco, le nombre total d'événements entre janvier 2016 et octobre 2017 a presque quadruplé. Au cours des dernières années, les États et les entreprises financières ont commencé à se préoccuper de la cybersécurité[6] (Cisco, 2018). Les cyberattaques et les incidents de sécurité des systèmes d'information (SSI) peuvent nuire gravement à la réputation des clients et aux investisseurs. Cependant, des incidents de violation de données ou de fuites d'informations se produisent à tout moment, entraînant de graves conséquences financières et juridiques pour les institutions financière (Cisco, 2018). Au Québec, au moins neuf PME sur dix ont estimé avoir un bon niveau de protection contre les cyberattaques, selon un sondage mené par Devolutions au début de 2022. Cette confiance ne reflète malheureusement pas leur réel niveau de préparation. En effet, selon le sondage, environ la moitié d'entre elles avaient utilisé des outils de contrôle de base tels qu'un gestionnaire de mots de passe (57%), l'authentification à deux facteurs (54%) ou une formation en cybersécurité (48%)[7]. Et moins du tiers d'entre elles (32%) effectuaient fréquemment un audit de sécurité. Selon un sondage de KPMG sur les perspectives des chefs de la direction en octobre 2022, à peine plus de la moitié des dirigeants d'entreprise canadiens se disaient prêts à faire face à une cyberattaque (Venne, 2023).

Un autre sondage mené par Devolutions en collaboration avec l'AQT a interrogé des professionnels des TI et des décideurs de 75 PME québécoises, ainsi que 217 PME à l'échelle internationale entre mars et mai 2023. Seulement 29 % des entreprises québécoises consacrent entre 7 et 14 % de leur budget technologies de l'information à la cybersécurité, comparé à 51 % au niveau international.

[6] https://www.cisco.com/c/fr_ca/products/security/common-cyberattacks.html consulté : 2024-04-30 à 15 :17 :20

[7] https://blog.devolutions.net/fr/2022/06/maintenant-disponible-le-portait-de-la-securite-informatique-chez-les-pme-quebecoises-en-2022/ consulté : 2024-04-29 à 15:10:29

Les préoccupations concernant la confidentialité et la sécurité des données sont élevées, avec 78 % des répondants internationaux et 94 % des répondants québécois exprimant leur inquiétude. Seulement un quart des entreprises québécoises se sentent prêtes à répondre aux exigences de la loi 25 (12 % comparé à 20 % à l'international). Bien que la majorité des entreprises disposent d'une équipe dédiée à la cybersécurité, un répondant sur sept ne bénéficie d'aucune ressource spécialisée, ni en interne ni en externe. Un faible pourcentage d'entreprises au Québec consacrant une part recommandée de leur budget TI à la cybersécurité, comparé au niveau international. Les préoccupations concernant la confidentialité et la sécurité des données varient entre les répondants internationaux et ceux du Québec. De plus, une minorité d'entreprises québécoises se sentent prêtes à répondre aux exigences de la loi 25, avec un taux d'adoption des solutions de gestion des accès privilégiés (PAM) inférieur à la moyenne internationale[8].

Le réseau Internet se développe et se propage très rapidement à travers le monde à un tel point que « dans la première décennie du XXIe siècle, on est passé de 350 millions à plus de 2 milliards d'individus connectés à Internet dans le monde » (Schmidt & Cohen, 2014). Selon Statistique Canada, environ 20 % des entreprises canadiennes ont été victimes d'attaques informatiques en 2017 (Sarrazin, 2019). Cependant, il y a encore peu d'entre elles capables de se prémunir suffisamment contre ce risque. Les problèmes majeurs sont les coûts, la manque de connaissances et la complexité des procédés. Mieux vaut prévenir les coups car les conséquences sont d'énormes pertes. Les confusions financières liées au risque opérationnel ont augmenté et ont entraîné d'énormes pertes financières, le risque opérationnel fait l'objet d'une prudence particulière de la part des autorités réglementaires, des banquiers et de la recherche universitaire (Haouat Asli, 2011).

[8] https://blog.devolutions.net/fr/2023/10/maintenant-disponible-le-portait-de-la-securite-informatique-chez-les-pme-quebecoises-en-2023-2024/ consulté le 2024-04-30 à 15 :00 :10

1.2 Cybersécurité, lois et règlements

1.2.1 Cybersécurité

La cybersécurité est l'ensemble des moyens utilisés pour assurer la sécurité des systèmes et de données informatiques d'un Etat et d'une entreprise (Guinchard, 2015).

Le domaine de la cybersécurité en 2024 est influencé par l'évolution constante des menaces en ligne, exigeant des solutions novatrices et adaptables. Pour faire face à ces défis avec succès, il est primordial de promouvoir la coopération internationale, de partager des informations concernant les menaces numériques, et de maintenir les investissements dans les dernières technologies de sécurité (Echoso, 2024). Confrontées à cette dynamique, les organisations doivent adopter une approche proactive et intégrée en cybersécurité, reconnaissant que cette dimension ne se résume pas uniquement à des problématiques techniques, mais revêt également une importance capitale dans la stratégie globale. En 2023, IBM a observé une augmentation de 40 % des cas d'atteintes à la sécurité associées à des intelligences artificielles malveillantes, mettant en lumière les aspects à la fois positifs et négatifs de cette avancée technologique. Echoso (2024) a analysé les technologies émergentes de renforcement de cybersécurité et a conclu que ces avancées technologiques tels que l'Internet des objets (IoT), le *cloud computing*, l'intelligence artificielle (IA), et la 5 G ont transformé le fonctionnement des entreprises et la vie quotidienne. Cependant elles ont également introduit de nouvelles vulnérabilités. La sécurité en ligne est devenue un problème crucial en raison de la croissance significative des attaques informatiques.

Selon une analyse de cybersécurité, les pertes liées à la cybercriminalité pourraient atteindre les 6 trillions de dollars par an dans le monde d'ici la fin de 2023, un chiffre qui continue d'augmenter en 2024 (Echoso,2024). Cette multiplication des risques est alimentée par la sophistication croissante des attaques et par la valeur de plus en plus élevée des données numériques.

La première évaluation des menaces cybernétiques nationales du Canada, publiée en 2018, a vu plusieurs de ses prédictions se concrétiser lors de ces deux dernières années. En 2020, cette évaluation arrive à un moment où les Canadiens se tournent de plus en plus vers les services en ligne, une transition accentuée par la pandémie de COVID-19. La crise sanitaire a souligné

l'importance vitale de protéger l'infrastructure numérique du Canada face à l'augmentation du télétravail, afin de garantir la sécurité nationale et l'épanouissement économique du pays (Khoury, 2023). Dans le cadre de son analyse des menaces cybernétiques nationales, Khoury (2023) a identifié des tendances concernant le paysage des cybermenaces et a présenté une vue d'ensemble de cinq thèmes qui influenceront les activités cybernétiques au Canada dans les années à venir.

L'étude de Bendovschi (2015) a mis en évidence que des entreprises de diverses tailles et secteurs ont été ciblées par des cyberattaques au cours des trois dernières années. Ces attaques touchent un large éventail de domaines, allant du secteur public (gouvernement, application de la loi, éducation, soins de santé) aux organisations à but non lucratif, en passant par les entreprises privées opérant dans la finance, les médias, les services en ligne, le tourisme, les télécommunications, la vente au détail, l'éducation, l'automobile et la sécurité. Une découverte intéressante mise en lumière par l'étude de l'auteur est que, lors de l'analyse des causes sous-jacentes des failles de sécurité, moins de la moitié des incidents sont attribuables à des attaques criminelles intentionnelles. Les formes d'attaques les plus courantes qui entraînent un accès non autorisé à des données comprennent la divulgation de renseignements tels que les noms complets, les dates de naissance, les identifiants personnels, les adresses complètes, les dossiers médicaux, les numéros de téléphone, les données financières, les adresses électroniques, les informations d'identification (noms d'utilisateur, mots de passe) et les informations d'assurance. La hausse des attaques informatiques a affecté les firmes financières, y compris *AXA Corporate Solutions Company*. Cette entreprise fait partie de celles ayant introduit une assurance visant à couvrir les dépenses liées à la remise en état post-cyberattaque, qu'il s'agisse d'un virus, d'une erreur ou d'un incident fortuit. Par ailleurs, elle a mis en place un produit spécialisé pour l'inspection, l'évaluation et la réduction des risques cybernétiques chez ses clients. Dans le domaine de la cybercriminalité et de la sécurité, un élément crucial réside dans le volet juridique. Les efforts constants s'opèrent pour l'élaboration des lois et des règlements afin de prévenir ou restreindre les activités criminelles en ligne. Mais la complexité réside dans le fait que ces cadres juridiques sont souvent délimités géographiquement, alignés avec des états ou régions spécifiques. Cela contraste avec la nature mondiale et internationale d'Internet, qui unit les individus à travers le monde sans frontières physiques (Bendovschi, 2015).

1.2.2 Protection des renseignements personnels

De plus en plus, des chercheurs, des experts provenant de grands cabinets de protection des renseignements personnels, ainsi que des autorités en matière de protection des renseignements personnels, s'intéressent à la gestion des risques liés à la protection des données personnelles (Fréminville, 2019). Cette attention accrue est due à la croissance de l'environnement de risque à l'échelle mondiale. Toutefois, les autorités en matière de protection des données personnelles utilisent le concept de vérification de protection des renseignements privés, qui englobe un ensemble de processus clairement définis (Tambou, 2020). Les autorités canadiennes de protection des renseignements personnels, notamment le Commissariat à la protection de la vie privée du Canada, sont responsables de promouvoir et de faire respecter la législation sur la protection des renseignements personnels au Canada, y compris dans le secteur bancaire. Ces autorités établissent des lignes directrices et des politiques pour assurer la protection des renseignements personnels détenus par les banques (OECD, 2002). Le Commissariat à la protection de la vie privée du Québec, en particulier, offre des ressources et des conseils pratiques aux institutions financières, y compris les banques, pour les aider à respecter leurs obligations en matière de protection des renseignements personnels. Ils encouragent la transparence dans la collecte, l'utilisation et la divulgation des renseignements personnels, ainsi que la mise en place de mesures de sécurité adéquates pour protéger ces informations (Levac, 2023). Il est important de noter que les réglementations liées à la protection des renseignements personnels dans le secteur bancaire peuvent varier en fonction des lois et des réglementations spécifiques à chaque province au Canada (Protection des renseignements personnels - Commission d'accès à l'information du Québec, 2012). En raison de l'importance accordée par les autorités chargées de la protection des renseignements personnels aux vérifications, on peut constater que celles-ci encouragent les entreprises à améliorer la gestion des risques liés à la protection des données privées. Nous vivons à l'ère de la surveillance généralisée où les gouvernements et les entreprises recueillent et scrutent nos données personnelles. Ces entités sont capables de tirer des conclusions à partir de l'analyse de ces données. Par exemple, Google possède une connaissance plus approfondie de nos pensées que nous-mêmes, car il conserve de façon permanente et très détaillée l'historique de nos recherches. Même si Google permet la personnalisation des préférences publicitaires, il ne nous accorde pas le droit de supprimer sélectivement les informations que nous ne souhaitons pas divulguer (Schneier, 2015).

Dans l'ouvrage innovant de Bruce Schneier (2015), une perspective inédite est offerte sur la confidentialité et la sécurité. Il souligne que Clay Shirky, un fournisseur de services de téléphonie mobile, aussi connu pour ses travaux dans le domaine des médias et de la technologie, effectue une surveillance étroite des déplacements et un accès à des informations sur les contacts. Les comportements d'achats en ligne et en magasin sont enregistrés, laissant transparaître des indices sur la situation professionnelle, la santé ou même une possible grossesse. Les messages échangés révèlent des éléments sur les relations intimes et occasionnelles. Google parvient à deviner des pensées en examinant des recherches confidentielles. Facebook peut déduire des éléments sur l'orientation sexuelle sans que la personne n'en ait parlé. Les entités surveillantes vont au-delà de la simple collecte de données. Les informations recueillies sont utilisées pour manipuler les contenus médiatiques et publicitaires, ainsi que pour ajuster les prix proposés. Les gouvernements utilisent la surveillance pour discriminer, censurer, restreindre la liberté d'expression et mettre des vies en danger à l'échelle mondiale. Ces entités partagent parfois ces données, et dans les situations les plus graves, des cybercriminels peuvent les exploiter lors de vastes violations de données. Une partie de cette surveillance est consentie et la collaboration avec la surveillance des entreprises est motivée par la promesse de commodité, tandis que l'acceptation de la surveillance gouvernementale est basée sur la perception de protection. Ce contexte a donné naissance à une société sous haute surveillance. Schneier (2015) propose une approche alternative valorisant la sécurité et la confidentialité. Il actualise son livre à succès avec une préface contenant les développements récents. Ensuite, il propose des actions concrètes pour réformer les programmes de surveillance gouvernementale, perturber les modèles économiques basés sur la surveillance et préserver la vie privée. Bensoussan (2018), souligne l'objectif principal du règlement européen sur la protection des données, qui vise à renforcer les droits des individus en matière de protection de leurs données personnelles et à faciliter la circulation fluide de ces informations sur le marché unique numérique. La collaboration entre les gouvernements, les entreprises et les experts est essentielle pour développer et utiliser l'IA de manière responsable et éthique tout en respectant les droits fondamentaux des individus (Akkour et al., 2023). La notion de stockage d'informations rejoint le principe baconien selon lequel la détention d'informations confère un certain pouvoir sur une entité ou un phénomène (Couldry & Mejias, 2020). La liaison entre le stockage d'informations et le principe baconien souligne comment la détention et le contrôle des connaissances peuvent être

des sources de pouvoir, influençant la dynamique sociale, économique et politique. Cela rejoint des préoccupations contemporaines sur la manière dont les données sont collectées, gérées et utilisées dans un monde de plus en plus axé sur l'information. Le lien avec la protection de la vie privée devient évident lorsqu'on considère l'impact de cette accumulation d'informations sur les individus. Richards (2022) souligne que : « La vie privée est une question de pouvoir car l'information est synonyme de pouvoir, et l'information vous donne le pouvoir de contrôler les autres personnes » (p.42). Il met en avant l'importance de protéger la vie privée non seulement pour préserver la dignité des individus, promouvoir leur autonomie ou défendre d'autres valeurs importantes, mais surtout pour contrer la disparité de pouvoir résultant de la collecte et de l'utilisation des informations personnelles par les entreprises, les gouvernements et les administrations publiques sur les consommateurs et les citoyens.

Finalement, Couldry et Mejias (2020), Richards (2022) et Akkour et al. (2023) ont penché leur recherche sur les meilleures pratiques en matière de protection des renseignements personnels.

Aubin (2023) observe que les entreprises font face à plusieurs défis lorsqu'il s'agit de s'adapter aux changements réglementaires en matière de protection des renseignements personnels. Elles doivent revoir et mettre à jour leurs politiques et procédures internes pour se conformer aux exigences plus strictes en matière de protection des renseignements personnels. Cela peut inclure des politiques de confidentialité plus détaillées, des protocoles de sécurité renforcés et des formations pour le personnel. Avec la numérisation croissante des services bancaires, les sociétés investissent davantage dans la cybersécurité qui consiste à renforcer les mesures de sécurité informatique pour protéger les données sensibles de leurs clients. Cela comprend la mise en place de pare-feu avancés, de cryptage des données et de systèmes de détection des intrusions. Les entreprises sensibilisent leur personnel à l'importance de la protection des renseignements personnels et mettent en place des programmes de formation pour les aider à reconnaître et à prévenir les risques de sécurité des données. Elles mettent en place des mécanismes de gouvernance des données plus rigoureux pour assurer une gestion responsable et éthique des données clients. Cela implique souvent la nomination d'un responsable de la protection des données et la mise en place de processus de suivi et de conformité (Aubin, 2023). La conformité aux nouvelles

réglementations en matière de protection des renseignements personnels peut engendrer des coûts importants en termes d'investissements dans la sécurité des données, la formation du personnel et la mise à jour des infrastructures informatiques. Les sociétés naviguent dans un paysage réglementaire complexe et en constante évolution, ce qui peut rendre difficile la mise en conformité totale avec toutes les exigences légales (Carbonneau, 2022). La gestion des risques s'avère indispensable pour assurer la sécurité et la confidentialité des données tout en permettant un accès rapide et facile aux services en ligne, ce qui peut être un défi délicat. Les entreprises doivent trouver un équilibre entre la protection des données et l'expérience client (Landreville, 2023). En résumé, les organisations fournissent des efforts importants pour s'adapter aux changements réglementaires en matière de protection des renseignements personnels en renforçant leurs mesures de sécurité, en sensibilisant leur personnel et en mettant en place une gouvernance des données plus stricte. Cependant, elles doivent relever des défis tels que les coûts supplémentaires, la complexité réglementaire et la gestion des risques pour assurer la conformité et la protection des données de leurs clients.

Comeau (2009) suggère que les autorités politiques, les représentants de la société civile, les citoyens et les gouvernements s'engagent dans une réflexion sur la question plus large de la protection de la vie privée et des informations personnelles, en favorisant un dialogue constructif entre les différentes parties prenantes dans la sauvegarde des données privées (Comeau, 2009). Les enjeux autour de la protection de la vie privée et des renseignements personnels continuent d'évoluer rapidement avec les progrès technologiques et les nouvelles exigences en matière de sécurité et de justice sociale. De nos jours, la protection des renseignements personnels est devenue une préoccupation majeure en raison de l'omniprésence des technologies de l'information. Les questions de confidentialité des données, de protection de la vie privée et de sécurité des renseignements personnels sont au premier plan. Les progrès rapides dans la collecte, le stockage et le partage des données ont soulevé des préoccupations croissantes quant à la sécurité et à la protection des informations personnelles (Nguyen, 2018). Des réglementations telles que le Règlement général sur la protection des données (RGPD) en Europe et d'autres lois sur la confidentialité dans le monde entier ont renforcé la protection des données personnelles. Les défis actuels incluent la sécurisation des données dans un environnement en ligne, la protection contre

les atteintes à la vie privée, et la gestion transparente des informations personnelles dans un monde de plus en plus connecté (Thibodeau, 2020). Les législations aux niveaux fédéral et provincial encadrant la protection des renseignements personnels définissent des critères pour identifier les informations couvertes par ces lois. Au niveau fédéral, la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) stipule que les renseignements personnels incluent toute donnée associée à une personne identifiable (Canada, 2021). Au niveau provincial, la Loi 25 qui modifie la Loi sur la protection des renseignements personnels dans le secteur privé (LPRPSP) offre une définition plus précise et restrictive. Selon cette loi, un renseignement personnel est une information qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier (Gouvernement du Québec, 2023). Ces deux lois canadiennes, fédérale et provinciale, englobent diverses catégories de renseignements personnels. Ils comprennent les caractéristiques fondamentales de l'individu, comme son nom, sa race, son origine ethnique, son âge, son poids, ses dossiers médicaux, son groupe sanguin, son ADN, sa religion, son état civil et son niveau d'éducation. Des éléments supplémentaires, tels que l'adresse électronique, les messages de courrier électronique, l'adresse IP (protocole Internet), les revenus, les habitudes de consommation, les informations bancaires telles que le numéro de compte en banque, les données de cartes de crédit et/ou de débit, les rapports de prêt ou de solvabilité, les déclarations de revenus et le numéro d'assurance sociale, sont également considérés comme étant des renseignements personnels selon ces lois (Rico, 2020).

Il est évident que les institutions doivent s'engager pleinement dans la protection des informations personnelles de leurs clients. Cet engagement est essentiel pour établir et maintenir la confiance des clients, et cela constitue également une obligation légale (Mattatia, 2021). Les conséquences d'une violation de la confidentialité des données personnelles peuvent être dévastatrices, tant pour les clients concernés que pour l'institution financière elle-même. Afin d'assurer une protection efficace des données personnelles, les entreprises doivent mettre en place des mesures de sécurité rigoureuses, comme la sensibilisation des employés, l'utilisation de protocoles de cryptage, et la mise en œuvre de politiques et de contrôles d'accès appropriés (Akkour, Assadi, et al., 2023). De plus, l'implication de l'audit interne dans l'évaluation de l'efficacité de ces mesures est cruciale pour assurer une conformité continue. Il est également important de reconnaître que la protection

des données personnelles est un domaine en constante évolution, et qu'il est nécessaire de mener des recherches afin de suivre les nouvelles tendances, technologies émergentes et les évolutions législatives. Les organisations doivent demeurer vigilantes et s'adapter à ces évolutions pour maintenir un niveau adéquat de protection des données personnelles (Dupont & Gagnon, 2008).

1.3 Divulgation de risques de cybersécurité par les organisations.

Une recherche menée par Calderon et Gao (2021) porte sur la relation entre la divulgation des risques de cybersécurité par les entreprises et les frais d'audit. En examinant des données de 2005 à 2018, il a été observé que les honoraires d'audit des entreprises sont influencés non seulement par la quantité d'informations fournies (nombre de mots), mais également par la clarté et le type de langage utilisé (lisibilité et terminologie litigieuse) dans leurs déclarations de risques de cybersécurité. Cette étude va plus loin que les recherches précédentes en montrant que les cabinets d'audit prennent en compte non seulement les incidents réels de cyberattaques, mais aussi la façon dont les risques de cybersécurité sont divulgués de manière générale. Cela suggère que les auditeurs intègrent la nature et le contenu des informations sur les risques de cybersécurité dans leurs évaluations des risques, et donc dans leurs structures de frais. En résumé, des informations plus faciles à lire peuvent conduire à une diminution des frais d'audit et éventuellement d'autres coûts de surveillance encourus par les entités enregistrées auprès de la SEC (Calderon & Gao, 2021).

Une étude de Eijkelenboom et Nieuwesteeg (2021) sur la divulgation d'informations sur la cybersécurité dans les rapports annuels néerlandais du point de vue financier et économique. Ils ont débuté en passant en revue les exigences légales en matière de divulgation des informations sur la cybersécurité dans les rapports annuels. Ensuite, ils ont abordé les motivations derrière la divulgation d'informations sur la cybersécurité et son impact sur les parties prenantes et les actionnaires. Ils ont formulé des hypothèses sur la divulgation effective d'informations sur la cybersécurité et présenté un plan pour une étude empirique exploratoire. Leurs résultats montrent qu'au cours de l'année 2018, bien qu'il n'y ait pas d'obligation légale stricte, 87 % des entreprises mentionnent la cybersécurité ou des termes similaires dans leurs rapports annuels. Cependant, seules 4 entreprises sur 75 ont divulgué plus de six mesures spécifiques de cybersécurité, malgré le potentiel avantage socio-économique que cela représenterait. Certaines grandes banques et

agences de placement néerlandaises n'ont pas fourni d'informations précises sur leurs stratégies de cybersécurité, un aspect important étant donné leur vulnérabilité aux incidents de cybersécurité, ce qui compromet la protection des créanciers, des investisseurs et d'autres parties prenantes. Leur analyse vise à alimenter la discussion autour de la nécessité de l'autorégulation ou d'éventuelles obligations en matière de cybersécurité dans les rapports annuels en droit financier (Eijkelenboom & Nieuwesteeg, 2021).

Dans une autre étude de Lajili et Zéghal (2005), ces chercheurs examinent les informations divulguées concernant les risques dans les rapports annuels des entreprises canadiennes. L'objectif est d'analyser l'environnement actuel de divulgation des risques, ses caractéristiques et l'utilité analytique de ces informations pour les acteurs de l'industrie canadienne. En utilisant la méthode de l'analyse de contenu, les auteurs décrivent et analysent en détail le contenu des divulgations d'informations sur les risques des entreprises présentes dans le TSE 300. Ils regroupent et classent ces informations pour en structurer l'analyse. Les résultats indiquent que les divulgations sont fréquentes, résultant à la fois des divulgations obligatoires et volontaires liées à la gestion des risques. Cependant, l'analyse montre que la façon dont les risques sont évalués et divulgués manque d'uniformité, de clarté et de quantification, limitant potentiellement leur utilité. En conséquence, les auteurs suggèrent que pour l'avenir, il serait bénéfique que les divulgations des risques soient plus structurées et plus détaillées. Cela contribuerait à réduire le déséquilibre d'informations entre les gestionnaires de risques et les investisseurs. En d'autres termes, en rendant les informations sur les risques plus formelles et plus exhaustives, cela permettrait aux investisseurs d'avoir accès à des informations plus claires et complètes, ce qui réduirait les disparités d'informations entre les deux parties et améliorerait la transparence (Lajili & Zéghal, 2005a).

Selon Karfoul et Lamarque (2011), les rapports annuels des institutions financières canadiennes sont d'une importance cruciale pour évaluer leur performance financière et leur gestion des risques de manière approfondie et pour comprendre les activités, les résultats, les actifs et les passifs, ainsi que les orientations et objectifs stratégiques de ces institutions. Mettre en avant leur pertinence permet de mieux évaluer la solidité financière des banques, de mesurer leur rentabilité et de juger de leur capacité à gérer les risques. Ils soulignent à travers leurs idées que ces rapports annuels sont

également d'une grande importance pour les investisseurs, les actionnaires et les organismes de régulation, car ils facilitent la prise de décisions éclairées en matière d'investissement et permettent de veiller à la conformité réglementaire des banques. L'analyse des rapports annuels permet d'évaluer la performance globale des banques, d'identifier les tendances et les risques émergents, ainsi que de comprendre les stratégies adoptées pour faire face aux défis économiques et financiers (Karfoul & Lamarque, 2011).

Par ailleurs, ces rapports annuels contiennent souvent des informations sur les initiatives de responsabilité sociale et environnementale des banques, un aspect de plus en plus important pour les parties prenantes. Les rapports annuels des banques sont des outils essentiels pour comprendre leur performance financière, leur gestion des risques, ainsi que pour évaluer leur conformité réglementaire et leurs engagements en matière de responsabilité sociale et environnementale. La mesure de l'efficacité du Système de Contrôle Interne d'une banque est une question importante dans le cadre de l'analyse de la gestion des risques opérationnels des organisations bancaires (Branco & Rodrigues, 2006).

Karfoul et Lamarque (2011) ont souligné qu'à ce jour, il n'existe pas de méthodologie ou de dispositif d'évaluation standardisé pour évaluer les contrôles effectués au sein des établissements financiers dans le cadre du contrôle interne. Ainsi, dans le cadre de leur projet de recherche abordant la question de l'évaluation de l'efficacité du système de contrôle interne des banques, dans le but de lier différentes caractéristiques des organisations bancaires à leur efficacité dans la gestion des risques opérationnels, il a été nécessaire de mener une recherche-action visant à développer un outil d'évaluation basé sur les travaux de différents organismes professionnels ou universitaires, qui serviront de cadre théorique et conceptuel. Pour ce faire, ils se sont optés pour une démarche empirique, en se basant sur les informations recueillies dans les rapports annuels de 17 établissements financiers. Cette démarche a permis d'évaluer les progrès réalisés et les propositions de construction de l'outil, ainsi que de procéder à une première classification des banques en fonction de ce critère (Karfoul & Lamarque, 2011).

En résumé, afin de mesurer l'efficacité du système de contrôle interne d'une banque, il est important de développer un outil d'évaluation basé sur des travaux de recherche et de mener une analyse empirique en se basant sur les informations disponibles dans les rapports annuels des établissements financiers.

Dans le secteur bancaire, caractérisé par un environnement dynamique et concurrentiel, certaines banques sont incitées à s'engager dans des activités à risque afin d'augmenter leur rentabilité. Cependant, la négligence d'une gestion prudente et équilibrée entre le risque et la rentabilité peut entrainer des conséquences majeures sur la performance des banques et la stabilité globale du système financier. Ouchchikh et al. (2023) ont mené une étude d'évaluation d'impact de la gestion des risques sur la performance financière des banques à partir des données recueillies dans les rapports annuels de huit banques marocaines sur une période s'étendant de 2006 à 2020. Ils ont élaboré une mesure synthétique de la performance financière. Leurs principaux résultats démontrent que le risque de crédit, le risque de liquidité et le risque opérationnel (Phishing, non-conformité réglementaire, attaques de logiciels malveillants, piratage informatique, vulnérabilités des systèmes, erreurs humaines etc.) exercent une influence significative et négative sur la rentabilité des banques marocaines. Ainsi, une gestion efficace de ces risques permet d'améliorer sensiblement la performance financière des banques et de garantir la durabilité du secteur bancaire nationale (Ouchchikh et al., 2023). En somme, il est crucial pour les banques marocaines de gérer ces risques de manière efficace afin de préserver leur performance financière et d'assurer la pérennité du secteur bancaire dans son ensemble.

1.4 Audit interne et cybersécurité

1.4.1 Pratique d'audit interne dans les organisations

Le terme « audit » trouve son origine du mot latin « audire », qui signifie « écouter ». En 1977, l'International Federation of Accountants (IFAC) a été créée dans le but de renforcer la profession comptable à l'échelle mondiale. Depuis 1996, l'IFAC se consacre au développement et à la promotion de la profession comptable afin qu'elle puisse offrir des services de haute qualité au public (Colasse, 2004). Ce processus a initié la recherche d'un rôle adéquat pour l'audit interne. Avec l'évolution des projets, il est devenu essentiel d'élargir le champ d'action de l'audit interne

pour en faire un outil de contrôle et d'évaluation de l'efficacité des méthodes de gestion et d'information de la direction (Belkacemie, 2017). Plusieurs facteurs clés ont contribué à cette évolution, notamment le besoin de déceler les erreurs et les fraudes, la multiplication d'organisations ayant des succursales dispersées géographiquement, ainsi que l'impératif d'obtenir des rapports périodiques précis et fiables. L'audit est généralement défini comme une démarche systématique et méthodique entreprise par des experts dans le but d'évaluer et de juger de manière objective et indépendante les systèmes et les procédures d'une organisation. Il repose sur l'utilisation d'une variété de techniques d'information et d'évaluation, conformément aux normes de l'évaluation, de l'appréciation, de la fiabilité et de l'efficacité (Collins & Valin, 1992). La définition de l'audit interne a naturellement le même but que celle-ci, Germond et Bonnault (1987) l'audit interne: « est un examen technique rigoureux et constructif auquel procède un professionnel compétent et indépendant en vue d'exprimer une opinion motivée sur la qualité et la fiabilité de l'information financière présentée par une entreprise au regard de l'obligation qui lui est faite, de donner en toutes circonstances, dans le respect des règles de droit et des principes comptables en vigueur, une image fidèle de son patrimoine, de sa situation financière et de ses résultats ». Ces domaines incluent l'efficacité et l'efficience des opérations, la fiabilité des rapports financiers ainsi que la conformité aux lois et réglementations en vigueur (« COSO », 2023). L'audit interne peut aussi être décrit comme une approche structurée de la gestion d'une entité, nécessitant la mise en place d'un système complexe. Ce système comprend diverses activités opérationnelles, fonctionnelles et administratives, qui sont conçues pour apporter de la valeur en fonction des besoins internes et externes. De plus, il comprend des systèmes d'audit interne adaptés aux objectifs et aux risques spécifiques des activités de l'entité. Il repose sur un personnel compétent et intégré, organisé selon une structure adéquate. Enfin, il repose sur des systèmes d'information et de données qui permettent de surveiller et d'évaluer les performances de l'entité.[9]

Le rôle principal de l'audit interne consiste à prévenir toute menace susceptible de perturber les opérations de l'entreprise avant même qu'elle ne se produise. Cela se fait en renforçant le système de contrôle interne (Renard, 2017). Son objectif n'est pas d'améliorer n'importe quel aspect, mais

[9] https://www.partagedesconnaissancesbw.be/attachment/425256/ consulté le 2024-08-24 13 : 24 :46

de s'assurer que le domaine audité est constamment en adéquation avec son environnement extérieur et qu'il accomplit efficacement sa mission assignée (Mouqin, 2008).

Dans le contexte de la gestion des risques, le rôle fondamental de l'audit interne est de fournir à la direction et au conseil l'assurance de l'efficacité de la gestion des risques. De cette manière, l'audit interne assure la préservation de l'indépendance et de l'objectivité de ses services d'assurance (Manfouo, 2023). L'auditeur interne exerce ses fonctions au sein de son entreprise, en collaboration avec l'ensemble des responsables, conformément aux orientations de la direction à laquelle il est rattaché et à laquelle il rend compte (Villalonga, 2011). Il dispose d'objectifs, de principes et de documents qui guident l'exercice de sa profession. L'audit interne poursuit en permanence deux objectifs principaux : d'abord, il s'assure que la direction applique correctement ses politiques et directives, ainsi que la qualité du contrôle interne. Ensuite, il aide les responsables concernés à améliorer leur niveau de contrôle et leur efficacité en les conseillant et en leur fournissant des recommandations (Boutemadja, 2013).

L'objectif de l'audit interne consiste à soutenir les membres de l'entreprise dans l'exercice de leurs responsabilités en leur offrant des avis et des recommandations sur les activités examinées, et en contribuant à l'amélioration du fonctionnement de l'entreprise. L'auditeur interne veille alors à l'efficacité du système de contrôle interne en s'assurant de son existence, en surveillant son fonctionnement, en proposant des recommandations pour son amélioration et en informant de manière indépendante la direction générale, l'organe délibérant et le comité d'audit sur l'état du contrôle interne (Sardi, 2002). Effectivement, les objectifs de l'audit interne peuvent être détaillés en cinq apports (Uwamahoro, 2022) : Assistance et conseil au management qui consiste à fournir une assistance et des conseils à la direction et aux responsables de l'entreprise pour améliorer leur prise de décision, renforcer les processus de gouvernance et atteindre les objectifs fixés (Schick & Lemant, 2001). Promotion de la culture de contrôle pour sensibiliser l'ensemble des collaborateurs à l'importance du contrôle interne et encourager une culture d'excellence en matière de gestion des risques et de conformité (Sarens & De Beelde, 2006). Accompagnement des changements afin de contribuer à la réussite des projets de transformation et d'évolution de l'entreprise en évaluant les risques associés, en recommandant des mesures d'atténuation et en veillant à la mise en œuvre de

bonnes pratiques. Prévention des difficultés qui permet d'identifier, d'évaluer et de prévenir les risques pouvant impacter négativement l'entreprise, afin de minimiser les difficultés et les pertes financières qui pourraient en découler. Et enfin révélateur d'amélioration qui consiste à identifier les opportunités d'amélioration des processus, des pratiques opérationnelles et des performances de l'entreprise, en proposant des recommandations pour optimiser son fonctionnement global et assurer sa pérennité (Mouqin, 2008). En poursuivant ces cinq apports, l'audit interne contribue à renforcer la gouvernance, la maîtrise des risques et l'efficacité opérationnelle de l'entreprise. « L'audit Interne est une activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée »(Lamkaraf & Houria, 2019). En effet, l'audit interne est un outil essentiel du contrôle interne qui permet à l'entreprise de vérifier que ses politiques, procédures et activités sont en conformité avec les normes et réglementations en vigueur. Selon l*'European Confederation of Institutes of Internal Auditors* (ECIIA), l'audit interne vise à conseiller et à soutenir la direction pour garantir l'efficacité du contrôle en élaborant un plan d'action basé sur les risques, englobant les activités clefs et les systèmes majeurs de l'entreprise (ECIIA, 2005).

Dans une étude antérieure de Jawadi (2010), des lacunes dans l'audit et la gestion des risques ont été identifiées, conduisant à des pertes financières et même une crise financière. Cette étude a utilisé un questionnaire de 10 questions, administré à un échantillon de 35 personnes comprenant à la fois 15 professionnels et 20 universitaires. Les résultats ont révélé un manque de surveillance de la part des gestionnaires, des cas de fraudes ignorées et des retards dans les mesures prises. Il a été recommandé de mettre en place une stratégie de gestion des risques efficace, ainsi que des mécanismes d'indépendance entre les services et les contrôles (Jawadi, 2010).

Par ailleurs, une autre étude de Ruse et al. (2014) souligne que l'audit interne et la gestion des risques partagent un objectif commun : le contrôle des risques. Étant donné que le risque est omniprésent dans toute organisation, il incombe à la direction de le gérer. L'auditeur interne joue un rôle clé en évaluant l'efficacité des processus de contrôle interne, en proposant des formations, des solutions et des recommandations à la direction et au conseil d'administration (Ruse et al., 2014). L'exposition des entreprises aux risques est de plus en plus forte, notamment en cette

période de crise. L'instabilité des marchés, la faible visibilité sur les plans de charge et l'émergence de marchés de plus en plus concurrentiels font apparaitre des risques financiers, stratégiques, mais également légaux, réglementaires et de réputation[10]. Les affaires financières ayant secoué les banques publiques algériennes telles que Khalifa Bank, Union Bank, BCIA et BNA ont mis en lumière la nécessité de renforcer le contrôle interne, désormais perçu comme une solution pour divers problèmes latents, y compris les questions éthiques. L'audit interne joue un rôle clé dans la maîtrise des risques liés aux opérations bancaires. Son objectif est de soutenir l'entreprise pour maintenir un contrôle interne efficace, améliorer l'efficacité des processus de gouvernance bancaire et de gestion des risques (Bendjeddou et al., 2014).

Cette démarche d'audit interne est essentiellement chargée d'évaluer et d'assurer la conformité, l'efficacité et la qualité des processus opérationnels, des contrôles internes et de la gouvernance au sein d'une organisation. Elle implique généralement un examen approfondi des pratiques commerciales et des procédures pour s'assurer qu'elles sont alignées sur les objectifs de l'entreprise et les réglementations en vigueur. L'audit interne joue un rôle essentiel dans une organisation. Il consiste à évaluer et à améliorer l'efficacité des processus de gestion des risques, de contrôle et de gouvernance. Les auditeurs internes examinent les opérations de l'entreprise pour s'assurer qu'elles sont conformes aux politiques et procédures établies, identifient les zones à risque et proposent des recommandations pour les améliorer (Schick, 2007). En résumé, l'audit interne contribue à assurer une gestion efficace et efficiente des activités de l'entreprise, tout en minimisant les risques.

[10]https://apprendreconomie.com/audit-interne-et-gestion-des-risques/ consulté 2024-08-24 13 : 32 :19

1.4.2 Audit interne et protection des renseignements personnels

L'audit interne joue également un rôle crucial dans l'évaluation de la cybersécurité et la gestion des risques de renseignements personnels. Les normes et les cadres reconnus dans ce domaine fournissent un cadre reconnu pour examiner et évaluer les contrôles de sécurité, les processus et les pratiques en place dans les organisations, y compris les banques, afin de garantir la protection des données sensibles (Culioli et al., 2009). Les banques canadiennes sont tenues de se conformer à des normes spécifiques en matière de cybersécurité et de protection des renseignements personnels. Les exigences réglementaires sont établies par les organismes de réglementation financière. L'audit interne peut aider à déterminer si les banques respectent les normes règlementaires et à identifier les lacunes éventuelles en vue une amélioration continue. L'audit des normes de qualification et de fonctionnement permet d'assurer la fiabilité et la transparence des processus de sécurité des banques. Cela garantit aux parties prenantes internes et externes que des mesures adéquates sont en place pour protéger les renseignements personnels des clients et maintenir la sécurité des systèmes informatiques (Sinha et al., 2011). Les normes d'audit permettent de démontrer une compréhension approfondie des pratiques de sécurité informatique et de gestion des risques, ainsi qu'une reconnaissance de l'importance de garantir la protection des données sensibles dans le secteur bancaire (Aliyu et al., 2020).

Il existe diverses normes d'audit en matière de cybersécurité et de gestion des risques informatiques. La norme ISO/CEI 27002 présente un ensemble de bonnes pratiques pour la gestion de la sécurité de l'information, offrant des recommandations et des contrôles pour aider les entreprises à élaborer un cadre de sécurité solide pour préserver les données confidentielles (Culioli et al., 2009). La norme SSAE 18 / ISAE 3402 établit les critères pour les audits des systèmes informatiques et des contrôles de sécurité internes. Ces normes sont utilisées pour évaluer l'efficacité des mesures de sécurité de l'information au sein des organisations (Sinha et al., 2011). La norme PCI DSS (Payment Card Industry Data Security Standard) est principalement une norme de conformité, mais elle sert également de référence pour les audits de sécurité des systèmes de paiement et de protection des données de cartes de crédit (Shaw, 2009). La norme NIST SP 800-53 est un guide qui fournit un ensemble exhaustif de contrôles de sécurité et de pratiques recommandées pour les systèmes d'information fédéraux. Elle est couramment utilisée comme

référence pour les audits de sécurité informatique (Kurii & Opirskyy, 2022). Ces normes d'audit jouent un rôle essentiel dans l'évaluation et l'assurance de la conformité, de la solidité des mesures de sécurité et de la gestion des risques associés à la cybersécurité au sein des organisations.

Il existe également des normes de qualification et de fonctionnement relatifs à la cybersécurité (annexe1). La norme internationale ISO/CEI 27001 concerne les systèmes de gestion de la sécurité de l'information (SGSI). Elle établit les critères pour instaurer, déployer, maintenir et améliorer un système de gestion de la sécurité de l'information au sein d'une organisation (Netwrix, 2024). Le cadre de cybersécurité du *National Institute of Standards and Technology* (NIST) propose des directives et des meilleures pratiques pour aider les entreprises à renforcer leur posture de sécurité. Il se focalise sur les étapes du cycle de gestion des risques : Identifier, Protéger, Détecter, Répondre et Rétablir (Newhouse et al., 2017). Le Standard de Sécurité des Données de l'Industrie des Cartes de Paiement (PCI DSS) est une norme de sécurité des données pour les entreprises qui manipulent des informations de cartes de crédit. Son objectif est de sécuriser les données de paiement des clients contre les violations et les fraudes (Sulistyowati et al., 2020). Les Contrôles de Sécurité d'Internet du Center for Internet Security (CIS Controls) représentent un ensemble de bonnes pratiques en sécurité informatique visant à aider les organisations à mettre en place des mesures de sécurité efficaces pour protéger leurs actifs informatiques contre les menaces cybernétiques (Aliyu et al., 2020). Il serait intéressant de souligner que ces dernières normes permettent d'établir des fondements de sécurité solides, pour mettre en place des politiques et pratiques pertinentes, et pour garantir la protection des informations et des systèmes contre les risques liés à la cybercriminalité.

Cependant, la littérature scientifique concernant la gestion des risques liés à la protection des renseignements personnels est limitée. Les études existantes, telles que celles de Karfoul et Lamarque (2011), de Khalil et al. (2022), portent principalement sur les différents aspects liés à la gouvernance et au contrôle interne, bien que la protection des renseignements personnels puisse constituer un facteur de risque important pour les institutions financières. Comme Kablan et al. (2023) le soulignent, il serait impensable de nier l'impact de la protection des renseignements personnels sur les décisions de gestion au sein des institutions financières.

1.5 Problématique

La cybercriminalité est devenue un enjeu crucial pour la sécurité digitale dès les années 1970. Les premières activités de piratage informatique et d'exploitation de vulnérabilités ont donné naissance à une forme de criminalité inédite. À partir de 1978, les modifications législatives ont progressivement pris en compte la nécessité de combattre ces nouveaux délits liés à l'abus de la technologie (Holt et al., 2022).

Cependant, tel qu'observé par Reis et Henrard (2017), seul un petit nombre d'institutions intègrent des outils de gouvernance pour gérer efficacement les risques associés à la protection des renseignements personnels.

Akkour et al. (2023) notent que la sécurité des données est essentielle pour les banques pour garantir la confidentialité et l'intégrité des informations de leurs clients. La confidentialité et l'intégrité des données personnelles revêtent une importance cruciale pour les banques, en particulier dans un environnement numérique où les cybermenaces sont omniprésentes. Ces auteurs ont donné leurs avis sur comment ces deux aspects clés de la sécurité des données sont essentiels dans le contexte bancaire. La confidentialité des données personnelles des clients est essentielle pour garantir leur vie privée et protéger leurs informations sensibles contre tout accès non autorisé. Les banques détiennent des données financières, des identifiants personnels et d'autres informations confidentielles qui doivent être protégées afin d'éviter tout risque de vol d'identité, de fraude ou de préjudice financier pour les clients. L'intégrité des données garantit l'exactitude, la fiabilité et la non-altération des informations tout au long de leur traitement, leur stockage et leur transmission. Toute modification non autorisée des données peut nuire à la confiance des clients dans l'exactitude des informations fournies par la banque, entraînant des conséquences néfastes pour les opérations financières et la prise de décision. Une faille de sécurité peut entraîner des répercussions dévastatrices et avoir un impact significatif sur tous les aspects de l'institution financière (Akkour et al., 2023).

Les failles de sécurité dans les banques peuvent entraîner des conséquences graves sur plusieurs fronts, rendant crucial leur attention et leur prévention.

Tout d'abord, une violation de données peut engendrer une perte de confiance chez les clients et les investisseurs. Selon Iat (2020), cette confiance est essentielle pour maintenir des relations solides et durables, et sa rupture peut se traduire par une diminution de la fréquentation des agences et des retraits de fonds importants. La perception de la capacité de la banque à sécuriser les informations personnelles peut dissuader de nouveaux clients et investisseurs.

Ensuite, les banques sont susceptibles de subir d'importantes pertes financières. Iat (2020) souligne que les coûts directs incluent le renforcement de la cybersécurité, l'embauche de professionnels pour gérer la crise, et les frais de communication avec les clients. En outre, les procédures judiciaires liées aux recours des clients peuvent engendrer des frais juridiques élevés. La diminution de la clientèle due à des préoccupations quant à la sécurité peut également entraîner une baisse des dépôts, affectant ainsi les résultats financiers à long terme.

De surcroît, les banques peuvent faire face à des amendes réglementaires en cas de non-conformité aux normes de sécurité des données. Ces sanctions, fixées par les autorités compétentes, visent à compenser les dommages causés aux individus et à dissuader de futures infractions (Solove, 2005).

Les atteintes à la réputation sont également un point critique. Une faille de sécurité, accompagnée de publicité négative, peut ternir l'image de l'institution, suscitant méfiance et fuite des clients vers des concurrents jugés plus sûrs. Cela peut compromettre la viabilité et la position de la banque sur le marché.

Enfin, les conséquences juridiques, telles que les litiges et les sanctions réglementaires, peuvent s'avérer coûteuses. Les clients affectés peuvent intenter des actions en justice, tandis que les autorités peuvent imposer des amendes significatives pour non-respect des réglementations.

Ainsi, il est impératif que les banques mettent en place des mesures de sécurité rigoureuses pour prévenir les violations de données et en atténuer les impacts financiers, juridiques et réputationnels.

En étudiant le thème de la cybersécurité et de la gestion des risques liés aux informations personnelles dans le contexte des banques canadiennes, notre recherche vise à comprendre

comment les banques canadiennes divulguent les risques reliés à la protection des renseignements personnels et les stratégies défensives qu'elles mettent en place pour gérer ces risques. Plus spécifiquement, il s'agit de vérifier si les banques canadiennes inventorient et divulguent les risques liés à la protection des renseignements personnels dans leurs opérations, de recenser les risques liés à la confidentialité des renseignements personnels dans les banques, et de relever les mesures de sécurité mises en place pour protéger les données personnelles des clients.

Ainsi, notre travail contribuera à améliorer les politiques et les pratiques de gestion des risques dans le secteur bancaire canadien, permettant ainsi de garantir la confidentialité et l'intégrité des données des clients et de renforcer la confiance du public dans le système financier du pays.

1.6 Questions de recherche

Dans le cadre de notre étude sur la gestion des risques liés à la protection des informations personnelles dans le secteur bancaire canadien, nous avons identifié deux questions de recherche centrales, qui sont toutes deux liées à la théorie de la signalisation, ainsi qu'à notre cadre conceptuel des risques. Ces questions serviront à préciser les objectifs de notre recherche et à illustrer comment cette théorie et ce cadre orientent notre analyse.

Question de recherche 1 : Comment les banques canadiennes utilisent-elles la divulgation proactive des risques associés à la protection des renseignements personnels comme un moyen efficace de renforcer la confiance des clients et des investisseurs ?

Cette question met en évidence l'importance d'une communication claire et transparente de la part des institutions financières. En s'appuyant sur la théorie de la signalisation décrite par Dainelli et al. (2013), nous examinerons comment la divulgation d'informations pertinentes concernant les risques de cybersécurité et les mesures d'atténuation peut agir comme un signal positif pour les parties prenantes. Plus précisément, nous chercherons à comprendre comment cette divulgation proactive peut réduire les incertitudes entourant la sécurité des données personnelles, influençant ainsi la perception des clients et des investisseurs quant à la fiabilité et la solidité de la banque. Nous explorerons également comment cette stratégie de communication peut accroître la fidélité des clients et attirer de nouveaux investisseurs, en créant un environnement de confiance essentiel

pour le fonctionnement efficace des établissements bancaires dans un paysage numérique complexe.

Question de recherche 2 : En quoi les stratégies adoptées par les banques canadiennes pour identifier, évaluer et gérer les risques liés à la protection des renseignements personnels améliorent-elles leur capacité à faire face aux cybermenaces ?

Cette question cherche à approfondir la compréhension des mécanismes concrets de gestion des risques que les institutions financières adoptent pour protéger les données sensibles de leurs clients. En utilisant le cadre conceptuel des risques selon Hubbard et Seiersen (2023), nous examinerons les processus systémiques mis en place par les banques pour identifier les vulnérabilités potentielles, évaluer leur probabilité et leur impact, et développer des stratégies d'atténuation adaptées. Nous prêterons une attention particulière aux normes de sécurité appliquées, telles que l'ISO 27001, ainsi qu'aux efforts de formation et de sensibilisation du personnel. À travers cette analyse, nous viserons à déterminer comment une approche proactive et structurée en matière de gestion des risques peut renforcer non seulement la sécurité des données, mais également la pérennité et la réputation des institutions dans un contexte où les menaces cybernétiques sont omniprésentes.

En résumé, ces deux questions de recherche guideront notre enquête en intégrant les principes de la théorie de la signalisation et de notre cadre conceptuel des risques. Ceci permettra de mieux comprendre comment les banques canadiennes naviguent dans le complexe paysage de la cybersécurité tout en protégeant les données personnelles de leurs clients. Ces analyses contribueront à éclairer les dynamiques de confiance et de sécurité au sein du secteur bancaire, offrant ainsi des perspectives significatives pour les politiques et pratiques futures.

1.7 Conclusion

D'après la littérature existante, la plupart des recherches académiques portent sur des sujets internationaux. De plus, les recherches Wa Mandzila et Zéghal (2009), Lajili & Zéghal (2005), Côté-Freeman (2019) mettent en évidence les risques les plus élevés liés à la protection des données personnelles, tels que l'atteinte à la vie privée, la collecte excessive de données, la vulnérabilité des systèmes de stockage, et les faiblesses des processus de contrôle interne mis en place par les

dirigeants. Ainsi, il est crucial de mettre en œuvre une gestion efficace des risques liés à la protection des données personnelles au sein des entreprises, en s'appuyant sur des professionnels qualifiés en sécurité informatique et en protection des données, tout en favorisant la coordination entre les différents services afin de faire face aux risques en temps opportun (Pesqueux, 2003). Un tel processus de gestion permettrait d'identifier, d'évaluer, et de corriger ces risques.

Cependant, au niveau des recherches menées au Canada, ces dernières sont peu nombreuses, voire presque inexistantes. Les informations recueillies proviennent principalement des sites de Statistique Canada, de revues spécialisées dans la protection des données et du rapport annuel sur la protection des données. En tenant compte de ces informations, il est primordial d'assurer la transparence et l'application des lois relatives à la protection des données personnelles afin de prévenir toute violence.

CHAPITRE 2
CADRE THÉORIQUE

Le secteur bancaire canadien traite une grande quantité de données financières et sensibles sur les citoyens. À mesure que la technologie numérique et les transactions en ligne deviennent de plus en plus répandues, les institutions financières sont exposées à des menaces et à des risques accrus liés à la cybersécurité et à la protection des données (Eddine & Ouassim, 2023). À cet effet, le présent travail revêt une importance particulière dans le domaine de la cybersécurité et la gestion des risques de données personnelles dans les banques canadiennes. Ce chapitre vise à aborder la théorie de la signalisation, le cadre conceptuel des risques liés à notre étude, qui établit les bases théoriques et les principes associés à l'identification et à l'évaluation des risques, et la gestion des risques, qui se concentre sur l'application pratique de ces concepts pour minimiser les menaces pesant sur l'organisation.

2.1 La théorie de la signalisation

Les relations commerciales reposent sur l'établissement de liens dynamiques et mutuellement bénéfiques entre entreprises ou individus, facilitant une variété d'échanges et de transactions. Ces interactions sont régies par un ensemble complexe de règles et de conventions, où la confiance joue un rôle crucial. Dans ce contexte, les décisions prises par les acteurs économiques ne peuvent se faire au hasard ; elles s'appuient sur des critères fondamentaux tels que la qualité, la fiabilité et la pertinence des informations disponibles (Armstrong et al., 2010). Pour garantir des transactions justes, stables et avantageuses pour toutes les parties impliquées, il est impératif que les choix soient réfléchis et fondés sur une analyse rigoureuse des données à disposition. Les entreprises qui souhaitent se différencier dans un marché concurrentiel doivent être particulièrement attentives à la manière dont elles communiquent leurs informations. En effet, la capacité à fournir des données transparentes et pertinentes devient un signal clé pour les investisseurs et les clients, leur permettant d'évaluer avec précision la santé économique et les performances morphologiques de l'entreprise. Selon Spence (1973), la théorie de la signalisation postule que cette communication d'informations n'est pas simplement une formalité, mais un levier stratégique. Elle permet de réduire les asymétries d'information, une situation dans laquelle une partie possède plus ou de meilleures informations que l'autre, pouvant ainsi nuire à l'équité des transactions. Par conséquent, les choix

d'une entreprise de divulguer certaines informations peut avoir des répercussions significatives sur sa réputation, sa crédibilité et, par extension, son succès sur le marché. Dans un environnement commercial où la concurrence est constante et où les attentes des parties prenantes évoluent rapidement, la capacité à envoyer des signaux pertinents et fiables devient incontournable. Ainsi les consommateurs attribuent une meilleure réputation aux entreprises qui communiquent largement sur elles-mêmes (Fombrun, et Van Riel, 2004). Cela implique non seulement la diffusion d'informations financières, mais également la communication sur les pratiques de la gestion des risques, les stratégies d'innovations, et l'engagement envers des pratiques éthiques et responsables. Ainsi, les entreprises qui adoptent une approche proactive en matière de signalisation ont tendance à renforcer leur position sur le marché, promouvoir la confiance des parties prenantes et optimiser leurs performances à long terme.

2.1.1 Importance de la communication d'informations pertinentes

La communication d'informations fiables et pertinentes est cruciale pour la santé financière et la réputation d'une entreprise. Le rapport annuel, en tant que document phare, représente un outil fondamental pour transmettre la performance de l'entreprise aux parties prenantes. Sa vérification rigoureuse, comme le soulignent Botosan et Plumlee (2002), renforce sa crédibilité et permet de garantir la qualité des informations fournies. Dans le cadre de la théorie de la signalisation, les dirigeants doivent comprendre que la manière dont ils communiquent les informations peut influencer la perception des investisseurs. Une communication proactive et transparente permet non seulement de prévenir les déséquilibres d'information, mais elle joue également un rôle essentiel dans la réduction des effets délétères associés à la sélection adverse (Dainelli et al., 2013). En fournissant des données précises et en les exposant de manière claire, les entreprises envoient un signal fort de leur solidité financière et de leur intégrité opérationnelle. Cette transparence, qu'elle soit financière ou opérationnelle, ne se limite pas à une obligation d'information, mais s'inscrit dans une stratégie visant à renforcer la confiance des investisseurs. En réduisant les incertitudes inhérentes à leurs décisions d'investissement, une communication efficace crée un environnement propice à la mobilisation des ressources et à la fidélisation des investisseurs, ce qui est essentiel pour la croissance à long terme de l'entreprise. Ainsi, non seulement une divulgation proactive d'informations pertinentes renforce la réputation de l'entreprise, mais elle agit également

comme un puissant levier pour attirer de nouveaux investisseurs, garantissant ainsi une base solide pour l'avenir.

2.1.2 Cadre théorique de la théorie de la signalisation

La théorie de la signalisation, telle que décrite par Dainelli et al. (2013), met en lumière l'importance de la communication proactive pour façonner la perception des parties prenantes concernant la santé financière et les performances d'une entreprise. Cette théorie repose sur l'idée que les informations transmises par une entreprise servent de signaux aux investisseurs et autres parties prenantes, leur permettant d'évaluer la qualité et la fiabilité d'une entreprise. Dans le contexte de notre étude sur la cybersécurité et la protection des données dans les banques canadiennes, il est essentiel d'explorer comment ces institutions communiquent non seulement les risques associés à la confidentialité des données, mais aussi les mesures proactives qu'elles adoptent pour atténuer ces risques. En analysant les stratégies de signalisation mises en œuvre par ces banques, nous serons en mesure d'évaluer l'impact de cette communication sur la confiance des clients et des investisseurs. Cette exploration doit inclure une évaluation des canaux utilisés pour faire passer l'information, des messages clés diffusés, et de la fréquence de ces communications. En effet, une signalisation efficace peut renforcer la transparence et la crédibilité des institutions financières, favorisant un climat de confiance qui est essentiel pour maintenir les relations avec les clients et attirer des investissements. En somme, comprendre comment les banques canadiennes gèrent leur communication sur les risques de cybersécurité et les protocoles de protection des données revêt une importance particulière non seulement pour la sécurité opérationnelle, mais aussi pour la perception de leur solidité et de leur responsabilité sociale. Cela souligne la pertinence de la théorie de la signalisation dans ce domaine spécifique, affirmant que des pratiques de communication réfléchies peuvent significativement influencer la confiance et la loyauté des parties prenantes envers une entreprise.

2.1.3 Divulgation et implications dans le secteur bancaire

La divulgation d'informations joue un rôle central dans les relations commerciales, favorisant la transparence et permettant aux parties prenantes de prendre des décisions éclairées. Dans le secteur bancaire, où la gestion des données personnelles est cruciale, il est impératif de comprendre comment les banques canadiennes abordent la divulgation des risques. Comme l'indiquent Alford (2002), la divulgation peut également comporter des risques, tels que la révélation d'informations

sensibles pouvant entraîner des conséquences imprévues, comme des litiges ou des atteintes à la réputation.

Pour cette raison, il est essentiel de trouver un équilibre entre la transparence et la protection des informations confidentielles. Les banques doivent naviguer avec précaution dans la communication des informations concernant leur performance et les risques associés à la cybersécurité. Cela comprend non seulement l'examen de la clarté et de la transparence de leurs rapports, mais aussi une évaluation critique de leurs pratiques de divulgation des risques.

Selon la théorie de la signalisation, comme le souligne Dainelli et al. (2013), les entreprises peuvent renforcer leur crédibilité et leur réputation en communiquant des informations pertinentes et de manière proactive. Dans le cas des banques canadiennes, des pratiques robustes de divulgation des risques peuvent envoyer des signaux positifs aux clients et investisseurs, leur permettant de mieux évaluer la solidité financière et la responsabilité de ces institutions. Les institutions financières doivent donc mesurer attentivement leurs stratégies de communication. Une divulgation réfléchie sur la gestion des risques associés à la cybersécurité non seulement répond aux exigences réglementaires, mais est également essentielle pour établir la confiance. Cela rassure les parties prenantes sur la capacité de la banque à protéger les informations de ses clients et à répondre efficacement aux menaces potentielles. Il devient primordial d'évaluer comment les banques canadiennes utilisent la divulgation comme un outil stratégique pour non seulement garantir la légitimité de leurs opérations, mais également pour construire une réputation forte et durable dans un environnement financier en constante évolution.

2.2 Cadre conceptuel

Le cadre conceptuel des risques constitue un cadre essentiel pour comprendre et gérer les incertitudes auxquels une organisation peut être confrontée. Son approche systématique se concentre sur l'identification, l'évaluation et la hiérarchisation des risques, ce qui permet aux gestionnaires d'obtenir une vision claire des menaces potentielles et des opportunités susceptibles de les affecter (Mun, 2012). L'objectif majeur de ce cadre est de minimiser les impacts négatifs des dangers identifiés tout en capitalisant sur les occasions favorables. En d'autres termes, ce cadre vise à protéger les actifs d'une organisation contre des événements indésirables, comme des pertes

financières, des atteintes à la réputation ou des violations de la conformité, tout en saisissant des opportunités qui peuvent favoriser la croissance et l'innovation (Aven, 2016).

Le processus du cadre conceptuel des risques est rigoureux et comprend plusieurs étapes clés. La première étape, l'identification des risques, consiste à définir et détecter les risques à travers des méthodes telles que les questionnaires, les entretiens avec les parties prenantes et l'analyse des données historiques. Une identification systématique et exhaustive permet de créer une base solide pour les étapes suivantes. Une fois les risques identifiés, il est crucial d'évaluer leurs probabilités d'occurrence ainsi que leurs impacts potentiels sur l'organisation. Cela permet de comprendre la sévérité des menaces et de prioriser les efforts de gestion (ISO 31000, 2018). Cette évaluation peut impliquer des méthodes qualitatives et quantitatives, telles que l'analyse par scénario ou l'analyse statistique.

Les risques doivent être classés en fonction de leur importance afin d'allouer efficacement les ressources pour traiter les risques les plus significatifs en priorité. Cette hiérarchisation garantit que l'organisation ne soit pas submergée par des problèmes mineurs tandis qu'elle ignore des menaces plus graves (Hillson, 2017). Pour chaque risque priorisé, il est essentiel de développer des stratégies d'atténuation adaptées. Ces stratégies peuvent comprendre l'évitement des risques, le transfert des risques (par exemple, à travers des assurances), la diminution des risques par le biais de contrôles internes, ou encore l'adoption de mesures correctives (Bromiley et al., 2016). Une fois les stratégies établies, leur mise en œuvre nécessite une coordination efficace des ressources humaines et matérielles. Parallèlement, un suivi continu est indispensable pour évaluer l'efficacité des mesures d'atténuation mises en place. Cela doit comprendre des revues régulières et des adaptations face à l'évolution des circonstances (Allen, 2003).

Dans un monde où les menaces évoluent rapidement, notamment en ce qui concerne la cybersécurité et la protection des données, l'intégration du cadre conceptuel des risques dans les pratiques organisationnelles est plus pertinente que jamais. Les entreprises doivent naviguer dans un paysage régulé où la conformité aux lois sur la protection des données, telles que le RGPD, devient une nécessité stratégique (Bénaroch, 2021). De plus, l'évolution technologique et la numérisation croissante des opérations imposent une réévaluation constante des risques associés, ce qui souligne l'importance d'une approche adaptable et proactive en matière d'analyse des risques. Cela est particulièrement vrai dans le secteur bancaire, où les données sensibles des clients

nécessitent des protections rigoureuses contre les cybermenaces et les violations de la confidentialité (Hubbard & Seiersen, 2023).

Le cadre conceptuel des risques représente un outil crucial pour les organisations cherchant à se défendre contre un éventail croissant de risques tout en capitalisant sur les opportunités qui se présentent. En se basant sur un cadre systématique et rigoureux, les entreprises peuvent non seulement réduire les impacts négatifs des menaces potentielles, mais également renforcer leur résilience face à un environnement en constante évolution.

2.2.1 Cadre théorique de risques

Selon Hubbard et Seiersen (2023), le cadre conceptuel de risques liés à la protection des renseignements personnels permet d'identifier, d'évaluer et de gérer efficacement les risques associés à la collecte, au stockage et à l'utilisation des informations personnelles. Cette approche est essentielle pour protéger les données sensibles contre de potentielles menaces, telles que le vol d'identité ou la violation de la vie privée. Les principes fondamentaux de l'analyse des risques incluent la sensibilisation à la confidentialité, la mise en place de mesures de sécurité adéquates, et la conformité aux réglementations, comme le Règlement Général sur la Protection des Données (RGPD).

Le cadre conceptuel de risques doit être envisagée dans un cadre plus large, qui intègre également des considérations de cybersécurité. Dans le secteur bancaire, les normes de sécurité sont primordiales pour assurer la protection des données sensibles (Taillat et al., 2023). Ainsi, il devient indispensable d'adopter une approche stratégique et holistique de la sécurité informatique, comprenant l'élaboration d'une politique de sécurité claire, la sensibilisation du personnel, et la mise en œuvre de mesures préventives et correctives (Cybersécurité - 5e éd., 2016).

2.2.2 Application pratique dans le secteur bancaire

Les banques canadiennes doivent impérativement adopter des stratégies robustes de gestion des risques pour se prémunir contre un éventail croissant de cybermenaces. Cela commence par une identification minutieuse des actifs critiques, tels que les données personnelles des clients et les transactions financières. En parallèle, l'évaluation des vulnérabilités dans les systèmes de gestion de l'information constitue une étape clé dans le renforcement de leur sécurité (Moisand & De

Labareyre, 2009). Un cadre reconnu comme l'ISO 27001 offre un socle structuré pour établir et maintenir un système de gestion de la sécurité de l'information (SMSI). En intégrant cette norme, les banques peuvent formaliser leurs processus de gestion des risques liés à la sécurité des données, ce qui leur permet d'implémenter des mesures de sécurité techniques et administratives adaptées à leurs besoins spécifiques. Ces mesures incluent la classification des données, l'accès restreint basé sur des rôles, et la mise en place de systèmes de détection et de réponse aux incidents.

Les risques associés à la protection des renseignements personnels proviennent de plusieurs sources. Parmi ceux-ci figurent le non-respect des lois et réglementations en matière de protection des données, la complexité des systèmes de collecte et de stockage des informations, ainsi que des lacunes dans les contrôles internes (Simonnet, 2015). Fort de cette réalité, les institutions financières doivent adopter une approche proactive, impliquant une surveillance continue et une mise à jour régulière de leurs pratiques pour s'assurer de leur conformité vis-à-vis des obligations légales.

Enfin, pour que les banques canadiennes renforcent leur résilience, il est crucial qu'elles établissent une culture de la cybersécurité au sein de leurs équipes. Cela nécessite une formation continue et une sensibilisation des employés aux risques liés aux données. En intégrant ces principes dans leur fonctionnement quotidien, les banques non seulement se conforment à des normes de sécurité élevées, mais favorisent également une approche collective de la protection des données, essentielle pour établir une confiance durable avec leurs clients et parties prenantes.

2.2.3 Évaluation et transparence dans la divulgation des risques

Dans un environnement de forte réglementation, notamment en matière de protection des données personnelles, la transparence des banques concernant les risques associés à ces données devient non seulement une obligation légale, mais aussi un impératif stratégique. La divulgation claire et précise des risques contribue de manière significative à instaurer un climat de confiance entre les institutions financières, leurs clients et autres parties prenantes (Luo & Naveen, 2006). Cette transparence permet aux clients de mieux comprendre les défis liés à la sécurité de leurs informations et de prendre des décisions éclairées sur l'utilisation des services bancaires.

La première étape dans ce processus consiste à identifier et évaluer systématiquement les risques auxquels les données personnelles sont exposées. Les banques doivent effectuer des analyses

approfondies pour déterminer non seulement les types de données qu'elles collectent, mais aussi les menaces potentielles, telles que les cyberattaques, les violations dues à des erreurs humaines ou des logiciels malveillants. Cette évaluation devrait également tenir compte des impacts potentiels sur la réputation et la performance financière de l'institution en cas de violation des données.

Une fois ces risques identifiés, les établissements doivent mettre en place des mesures de sécurité robustes. Cela inclut non seulement l'implémentation de technologies avancées, telles que le chiffrement des données, des systèmes de détection d'intrusion et des pare-feu sophistiqués, mais aussi le développement d'une culture de sécurité au sein de l'organisation. Par exemple, la formation continue des employés sur les meilleures pratiques de sécurité est essentielle pour minimiser les erreurs humaines, qui sont souvent à l'origine des violations de données. Des programmes de sensibilisation à la cybersécurité doivent être élaborés pour garantir que tous les membres du personnel, y compris ceux qui n'occupent pas des postes techniques, comprennent les enjeux et les responsabilités en matière de protection des données (Taillat et al., 2023).

En outre, une communication proactive sur les risques et les mesures de sécurité mises en place peut renforcer la perception de l'engagement des banques en matière de protection des données personnelles. Les banques peuvent choisir de publier des rapports de transparence réguliers, fournissant des informations sur les types de données collectées, les risques identifiés, les incidents de sécurité survenus, et les réponses apportées. Cette approche non seulement informe les parties prenantes, mais aussi les responsabilise dans le cadre de la gestion des risques associés aux données sensibles.

Enfin, il est crucial que les banques adaptent en permanence leurs pratiques de divulgation à l'évolution des réglementations et des attentes du marché. La conformité avec des législations telles que le Règlement Général sur la Protection des Données (RGPD) nécessite un engagement continu à évaluer et à améliorer les pratiques de divulgation et de gestion des risques. Par conséquent, les institutions financières doivent voir la transparence non seulement comme une obligation, mais comme un levier stratégique qui peut leur conférer un avantage concurrentiel dans un marché de plus en plus soucieux de la protection des données.

2.3 Gestion des risques liés à la protection des renseignements personnels et cybersécurité

Dans le contexte de la gestion des risques, Guedrib (2013) définit le risque comme une situation incertaine ayant un impact potentiel sur les objectifs d'une entité. Les risques liés à la protection des renseignements personnels englobent les menaces à la confidentialité, à la sécurité et à l'intégrité des informations individuelles, pouvant entraîner des violations de la vie privée (Cavoukian, 2023). Ces risques peuvent découler d'une mauvaise gestion des données, d'attaques informatiques ou d'autres incidents liés à la collecte et au stockage des données.

Rakotomandimby (2023) souligne que le risque lié à la protection des renseignements personnels survient lorsque la protection adéquate n'est pas assurée, et Trudel et Benyekhlef (1997) ajoutent que ce risque inclut la violation des règles de protection et le manque de connaissance des mesures appropriées. Les auteurs insistent sur le fait que la gestion de ces risques dépend fortement des pratiques adoptées par les institutions financières.

Bendovschi (2015) identifie trois principales sources de risques liés à la confidentialité des données : les attaques délibérées, les erreurs humaines et les failles du système. La complexité des cyberattaques rend la quantification des coûts et des répercussions difficiles, car les entreprises ne divulguent pas toujours toutes les informations pertinentes. Les conséquences peuvent inclure la perte de données, des perturbations d'activité et des dommages à la réputation.

La gestion des risques cybersécuritaires est devenue essentielle, particulièrement dans le secteur financier, où les risques sont en constante évolution (Barkat, 2017). Le cadre conceptuel de gestion des risques propose une approche stratégique qui intègre des méthodes d'analyse et de contrôle interne. Le référentiel méthodologique d'analyse du contrôle interne développé par le comité COSO (Committee of Sponsoring Organizations of Treadway Commission) aussi intègre la gestion des risques dans les processus stratégiques de l'entreprise. Un bon contrôle interne permet non seulement d'identifier les risques, mais aussi de mettre en place des mesures pour les gérer efficacement. Ainsi, la gestion des risques doit être perçue comme un processus holistique qui inclut sensibilisation, prévention des fraudes et adaptation aux nouvelles menaces (Gumb & Noël-Lemaître, 2007).

En somme, une gestion proactive des risques liés à la protection des renseignements personnels est cruciale pour garantir la sécurité des données dans un environnement numérique complexe,

renforçant ainsi la confiance des utilisateurs et contribuant à la résilience des institutions financières.

2.4 Conclusion

Ce chapitre a mis en lumière les enjeux importants auxquels se confronte le secteur bancaire canadien concernant la cybersécurité et la protection des données personnelles. En explorant la théorie de la signalisation décrite par Dainelli et al. (2013) et le cadre conceptuel de risques par Hubbard et Seiersen (2023), nous avons pu analyser comment ces concepts sont utilisés pour appréhender les méthodes de divulgation des risques et les approches de gestion mises en œuvre par les banques. L'importance d'une communication claire et proactive sur les risques liés à la protection des données s'est avérée fondamentale pour consolider la confiance des clients et des investisseurs. En tant qu'institutions dignes de confiance, les banques canadiennes doivent évoluer dans un environnement numérique en constante transformation, où les menaces cybernétiques sont omniprésentes. Gérer ces risques efficacement nécessite non seulement des solutions techniques, mais également une approche intégrée qui englobe l'évaluation des vulnérabilités, l'adoption de mesures de sécurité solides, ainsi qu'une sensibilisation continue des personnels. L'implémentation de normes de sécurité, comme l'ISO 27001, peut offrir un cadre robuste pour accroître la résistance des institutions financières face à ces dangers croissants. En définitive, notre étude souligne l'importance d'une amélioration constante des démarches de gestion des risques au sein des banques canadiennes. En analysant la clarté de leurs divulgations et l'efficacité de leurs systèmes de protection, nous contribuons à établir des fondations solides pour la confiance publique. Cette recherche met en avant la nécessité d'actions rapides dans un contexte où la protection des données personnelles représente non seulement une obligation réglementaire, mais également un enjeu stratégique pour maintenir la durabilité et la réputation des institutions bancaires à l'ère numérique.

CHAPITRE 3

METHODOLOGIE

Dans le cadre de cette étude, nous nous penchons sur la question fondamentale de la divulgation des risques liés à la protection des renseignements personnels par les banques canadiennes, ainsi que sur les stratégies défensives mises en place pour gérer ces risques. Pour répondre à cette problématique, nous avons choisi d'adopter une approche qualitative, qui s'avère particulièrement pertinente dans ce contexte. Selon Hammarberg et al. (2016), la recherche qualitative permet d'explorer en profondeur des phénomènes complexes et d'obtenir une compréhension nuancée des comportements et des perceptions des acteurs concernés. Les avantages de cette approche incluent la flexibilité et la richesse des données, ce qui est essentiel lorsque l'on s'intéresse aux discours des banques sur des sujets sensibles tels que la cybersécurité et la protection des données personnelles.

Les études antérieures sur la divulgation des risques ont souvent utilisé des méthodes qualitatives similaires, notamment l'analyse de contenu, l'entretien et l'analyse documentaire. Selon Leray (2008) et Bahl et al. (2021), l'analyse de contenu est particulièrement efficace pour examiner comment les organisations communiquent les informations sur la gestion des risques. Dans ce cadre, notre choix d'une méthode d'analyse de contenu est justifié par ces travaux qui montrent qu'elle permet d'identifier les thèmes récurrents et les approches adoptées par les organisations dans la divulgation des informations critiques.

Cependant, il est important de reconnaître que la recherche qualitative présente également des limites, notamment la subjectivité de l'analyse et la difficulté de généraliser les résultats à l'ensemble du secteur bancaire canadien. Par exemple, des études antérieures ont révélé que les résultats d'analyses qualitatives peuvent varier en fonction des biais des chercheurs (Noble & Smith, 2015).

Selon Leray (2008) et Bahl et al. (2021), l'analyse de contenu est une méthode de recherche qualitative qui permet d'explorer et d'interpréter des textes et des communications afin de dégager

des significations, des thèmes et des tendances. Cette approche est particulièrement efficace pour examiner comment les organisations transmettent des informations sur la gestion des risques, car elle permet d'analyser en profondeur les messages, les discours et les stratégies de communication déployées pour informer les parties prenantes des risques identifiés et des mesures prises. L'analyse de contenu aide ainsi à comprendre les nuances et les intentions derrière la communication organisationnelle.

Pour structurer notre analyse, nous avons retenu la méthode d'analyse de contenu. Cette méthode nous permettra d'examiner systématiquement les rapports annuels des banques canadiennes, en mettant en lumière les informations spécifiques liées à la cybersécurité, à la gestion des risques et à la protection des données personnelles. L'analyse de contenu est particulièrement adaptée à notre question de recherche, car elle nous offre la possibilité d'identifier les thèmes récurrents, les omissions potentielles et les nuances dans la manière dont les banques abordent la divulgation des risques.

Concernant notre échantillon, nous avons sélectionné un ensemble de rapports annuels des trente-quatre banques canadiennes pour les années 2020, 2021 et 2022. Au regard de la littérature existante, des études antérieures ont généralement utilisé des échantillons variants entre dix et cinquante organisations dans des contextes similaires (Ramboarisata et al., 2008). Notre échantillon de trente-quatre banques s'inscrit dans cette fourchette et nous semble approprié pour garantir une analyse représentative. Cependant, nous sommes conscients que la disponibilité et la qualité des informations divulguées peuvent varier d'une institution à l'autre, ce qui fait partie des difficultés inhérentes à notre recherche. De plus, dans un contexte marqué par un nombre croissant de cyberattaques et un manque de transparence concernant les incidents de cybercriminalité, il n'est pas possible d'établir un ensemble de données exhaustif pour une analyse plus approfondie.

Ainsi, ce chapitre méthodologique vise à justifier notre choix de recherche qualitative et à décrire en détail la méthode d'analyse de contenu que nous employons, tout en précisant la nature de notre échantillon. Ce faisant, nous nous efforcerons de mettre en lumière les pratiques des banques canadiennes en matière de divulgation des risques liés à la protection des renseignements personnels.

3.1 Méthode qualitative

La recherche qualitative est une approche méthodologique qui vise à comprendre les phénomènes sociaux en explorant les expériences, les comportements et les significations attribuées par les individus (Creswell & Creswell, 2017). Contrairement à la recherche quantitative, qui se concentre sur des données mesurables et des analyses statistiques, la recherche qualitative privilégie l'exploration approfondie des opinions, des perspectives et des contextes. Parmi les méthodes couramment utilisées en recherche qualitative, on trouve les entretiens, les groupes de discussion, l'observation et l'analyse de contenu, chacune offrant des façons différentes de recueillir et d'interpréter des données.[11]

Dans le cadre de notre étude de recherche sur la cybersécurité et la gestion des risques liés à la protection des renseignements personnels dans les banques canadiennes, notre objectif est de comprendre comment ces institutions divulguent les risques et mettent en place des stratégies défensives pour gérer ces enjeux. Plus spécifiquement, notre recherche se concentre sur l'inventaire et la divulgation des risques liés à la confidentialité des données personnelles, ainsi que sur l'évaluation des mesures de sécurité mises en place pour protéger les données des clients.

La méthodologie qualitative adoptée se concentrera exclusivement sur l'analyse des rapports annuels des banques pour examiner comment elles divulguent les risques liés à la protection des renseignements personnels et mettent en place des stratégies défensives pour gérer ces risques. Cette approche se base sur les informations contenues dans des documents publics accessibles et permettra d'explorer les pratiques de divulgation des risques liés à la protection des données privées spécifiques auxquels ces institutions sont confrontées. L'analyse de contenu, une méthode qualitative, sera utilisée ici, car elle nous permet d'extraire des thèmes, des motifs et des informations clés des rapports analysés.

Pour atteindre cet objectif, notre méthodologie qualitative s'appuie sur la théorie de la signalisation et le cadre conceptuel de risques. La théorie de la signalisation, selon Dainelli et al. (2013), elle

[11] https://scienceetbiencommun.pressbooks.pub/projetthese/chapter/methodes-qualitatives-de-recherche/ consulté 2024-08-24 16 : 18 :27

souligne l'importance de transmettre activement des informations afin de renforcer la confiance et minimiser les risques. Dans cette optique, nous analysons les rapports annuels des banques canadiennes afin d'évaluer comment la divulgation des risques influence la perception des investisseurs et des clients, soulignant ainsi l'importance de la transparence et de la communication proactive. La théorie de la signalisation, qui souligne le rôle de la transparence et de l'ouverture dans la divulgation des informations confidentielles, est pertinente dans le contexte de cette analyse des rapports annuels. Les arguments d'Alford (2002) mettant en lumière l'importance de l'équilibre entre la divulgation et la préservation de la confidentialité seront explorés à travers les informations divulguées par les banques canadiennes dans leurs rapports annuels. En lien avec le cadre conceptuel de risques, décrite par Hubbard et Seiersen (2023), qui met l'accent sur l'identification, l'évaluation et la gestion proactive des risques, cette analyse des rapports annuels examinera spécifiquement les risques liés à la confidentialité des renseignements personnels divulgués par les banques canadiennes. Mun (2012) souligne l'importance de minimiser les impacts négatifs des risques tout en capitalisant sur les opportunités, des éléments qui seront évalués à travers les informations disponibles publiquement dans les rapports annuels. L'analyse qualitative des rapports annuels permettra d'identifier les risques liés à la protection des renseignements personnels dans le contexte des banques canadiennes, tels que les cyberattaques, les lacunes en matière de sécurité des données et le respect des réglementations en matière de confidentialité. Cette démarche visera à tirer des conclusions significatives sur les pratiques de divulgation des risques et les stratégies défensives des banques canadiennes en matière de gestion des risques liés à la protection des données personnelles, en se basant uniquement sur les données disponibles dans les rapports annuels. En somme, cette méthodologie qualitative centrée sur l'analyse des rapports annuels des banques canadiennes offre une opportunité unique d'explorer les pratiques de gestion des risques et de divulgation spécifiquement liées à la protection des renseignements personnels, en se fondant sur des sources d'information accessibles au public.

3.2 Sélection des banques

La première étape a consisté à sélectionner trente-quatre des plus de soixante banques canadiennes et étrangères exerçant leurs activités au Canada et dont les rapports annuels sont analysés. La liste des banques provient de plusieurs sources, notamment, l'Association des banquiers canadiens et le

Bureau du surintendant des institutions financières[12]. Les critères de sélection sont basés sur la taille des institutions, leur expérience en cybercriminalité, leur envergure nationale ou internationale, ainsi que leur présence sur l'ensemble du territoire canadien. En vue de réaliser cette recherche qualitative, nous avons sélectionné les trente-quatre banques selon la méthode d'échantillonnage non probabiliste pour les raisons de temps et de coût. Nous estimons néanmoins que le nombre de trente-quatre banques permet d'assurer une représentativité de l'ensemble du secteur bancaire canadien. Ce nombre significatif de banques permet donc d'avoir une vision assez complète des pratiques en matière de cybersécurité et de gestion des risques liés à la protection des renseignements personnels dans le secteur bancaire.

Pour ce faire, nous avons sélectionné les six plus grandes banques à charte du Canada [13]. Ces institutions financières se positionnent en tant que leaders du secteur bancaire canadien compte tenu de leurs actifs. À la fin de 2022, elles détenaient 93 % de tous les actifs bancaires du pays. Elles jouent un rôle majeur dans le secteur financier canadien et ont une présence significative aussi bien sur le marché national qu'à l'échelle internationale. Elles offrent une gamme complète de services bancaires, investissements et produits. Il s'agit de :

[12] Selon l'Association des banquiers canadiens, il existe plus de 60 banques canadiennes et étrangères exerçant des activités au Canada, https://cba.ca/cba-today?l=fr, consulté le 22-08-2024 ; le Bureau du surintendant des institutions financières https://www.osfi-bsif.gc.ca/fr/surveillance/entites-reglementees consulté le 22-08-2024

[13] Selon Ian Bickis, « Pourquoi les six grandes banques canadiennes sont si dominantes », *La Presse canadienne*, 21 avril 2023. https://plus.lapresse.ca/screens/c20263dd-4ae7-40c8-b680-e5a9bc9f7acc%7C_0.html

Tableau 1 : Les six banques sélectionnées en raison de leurs actifs

Banques	
1	Banque Royale du Canada (RBC)
2	Toronto Dominion Bank (TD)
3	Banque Scotia (Scotiabank)
4	Banque de Montréal (BMO)
5	Banque Canadienne Impériale de Commerce (CIBC)
6	Banque Nationale du Canada

Nous avons également sélectionné, pour notre recherche, les vingt-huit banques ci-après en raison de leur expérience en matière de cybercriminalité et des incidents de cybercriminalité qu'elles ont traversées ainsi que leur implantation au Québec et dans d'autres provinces canadiennes :

Tableau 2 : Les vingt-huit banques sélectionnées en raison de leur expérience en matière de cybercriminalité et implantation au Québec et dans d'autres provinces

Banques			
1	Laurentienne	15	Canadian Western Bank
2	Desjardins	16	Banque de développement du Canada
3	Banque du Canada	17	Citizens Bank of Canada
4	Banque Alterna	18	General Bank of Canada
5	Banque Comerica	19	Versa bank
6	Banque JP Morgan Canada	20	Banque Peoples du Canada
7	HSBC Banque Canada	21	Banque RFA du Canada
8	Revolut	22	Banque Motus
9	Coast Capital	23	Banque Rogers
10	TangerineMD	24	Capital One
11	FirstOntario	25	Canada - Société Générale
12	Banque Équitable (EQ)	26	Caisses Populaires Acadiennes
13	Banque Manuvie Canada	27	Alberta Treasury Branches
14	Services financiers Le choix du Président	28	Citi Canada

3.3 Collecte des données

Pour notre recherche, nous avons principalement basé la collecte de données sur l'analyse des rapports annuels des trente-quatre banques canadiennes pour la période de 2020 à 2022. La période de 2020 à 2022 a été influencée par la pandémie mondiale de COVID-19, laquelle a eu un effet considérable sur les activités des banques, sur la cybersécurité et la protection des renseignements personnels. Les mesures de confinement et le passage au télétravail ont amplifié la vulnérabilité des systèmes d'information, augmentant ainsi les risques associés à la protection des données personnelles. L'étude de cette période permet d'examiner comment les banques canadiennes ont ajusté leurs stratégies de gestion des risques liés à la cybersécurité et de protection des renseignements personnels face à ces défis. Ces rapports contiennent des sections clés sur la cybersécurité, la protection des données personnelles, et la gestion des risques, qui sont essentielles à l'étude de la gestion des risques associés à la protection des renseignements personnels. L'analyse des documents, en particulier des rapports annuels, est une méthode largement reconnue dans la littérature académique. Selon Botosan et Plumlee (2002), cette approche permet d'évaluer la transparence et la responsabilité des organismes publics et privés, en offrant une perspective précieuse sur leurs pratiques de gestion des risques. De plus, l'étude de Chen et al. (2023) démontre que l'examen des rapports d'entreprises peut révéler des informations essentielles sur leurs politiques de cybersécurité, ce qui renforce la pertinence de notre méthode.

La collecte de données a été réalisée en suivant un processus systématique. Tout d'abord, nous avons organisé les documents en identifiant clairement chaque rapport par le nom de la banque et l'année tel que présenté à l'annexe 2. Ensuite, une lecture préliminaire a été effectuée pour obtenir une compréhension globale du contenu, en nous concentrant sur les sections relatives à la cybersécurité, à la gestion des risques, et à la protection des renseignements personnels. Cette première étape est cruciale pour identifier rapidement les informations pertinentes, comme le soulignent Hammarberg et al. (2016) et Patton (1987), qui insistent sur l'importance d'une lecture initiale attentive pour guider l'analyse détaillée. Après cela, nous avons élaboré un système de codage afin de structurer les données. Nous avons codé les informations concernant les risques liés à la protection des renseignements personnels, les conséquences potentielles associées, ainsi que les procédures de gestion des risques. Cette méthode de codage est conforme aux pratiques

recommandées dans la recherche qualitative par Valéau et Gardody (2016), qui affirment que le codage permet une analyse méthodique et rigoureuse des données collectées.

En approfondissant notre analyse, nous avons scruté les rapports pour dégager les mesures spécifiques de sécurité concernant les données personnelles, ainsi que les politiques établies par les banques pour protéger ces informations, comme le suggère un cadre d'analyse proposé par Familoni et Shoetan (2024). En outre, nous avons utilisé un système d'analyse comparative pour compiler et juxtaposer les informations extraites des rapports annuels, ce qui a permis d'identifier des tendances et des variances dans les pratiques des différentes institutions financières. Comme l'indique les recherches de Thomas et al. (2014) et Pickvance (2001), cette approche comparative est essentielle pour mettre en lumière les meilleures pratiques tout en révélant d'éventuelles lacunes.

Enfin, en consolidant les informations à l'aide de notre système de codage, nous avons pu annoter et regrouper les données pertinentes, notant les tendances, différences, et révélations significatives sur les protocoles de sécurité et leur variabilité d'une banque à l'autre. Cette analyse approfondie contribue à une meilleure compréhension des défenses relatives à la protection des données dans le secteur bancaire canadien.

3.4 Processus de codage

Pour structurer efficacement mon analyse, j'ai mis en place un système de codage qui me permet de classifier les informations pertinentes extraites des rapports annuels des banques. Ce processus de codage a été réalisé manuellement, en examinant attentivement chaque rapport pour extraire des données significatives et pertinentes. Je n'ai pas utilisé de logiciel d'analyse, car je considère que le codage manuel me permet une compréhension plus approfondie des nuances des informations présentées.

J'ai utilisé plusieurs catégories de codage, chacune ayant un objectif spécifique dans mon analyse. Les principales catégories comprennent :

1. Risques potentiels : Cette catégorie englobe toutes les mentions de situations où des données sensibles des clients pourraient être compromises en raison de failles de sécurité, d'attaques

malveillantes ou d'erreurs humaines. Par exemple, lorsqu'un rapport indique qu'une institution a subi une tentative d'accès non autorisé à son système de gestion des données personnelles, cette affirmation est codée sous le label "risques potentiels". Cela met en évidence les menaces qui pèsent sur la protection des renseignements personnels.

2. Mesures proactives : Cette catégorie inclut les initiatives de formation en matière de cybersécurité et tout programme mis en place par les banques visant à sensibiliser leurs employés aux meilleures pratiques en matière de sécurité des données. Par exemple, lorsqu'un rapport souligne que des employés ont suivi des formations spécifiques sur la prévention des cyberattaques ou sur la gestion des données sensibles, ces mentions sont documentées sous le code "mesures proactives". Ce codage est essentiel pour mettre en lumière les efforts d'anticipation et d'atténuation des risques entrepris par les banques pour protéger les informations de leurs clients.

3. Technologies de protection : Dans cette catégorie, j'ai attribué des codes aux mentions de technologies spécifiques mises en œuvre pour sécuriser les données. Cela inclut des techniques comme le chiffrement, l'utilisation de pare-feu, et d'autres solutions de sécurité qui protègent les données contre les accès non autorisés.

4. Incidents signalés : Cette catégorie englobe les références aux violations de données documentées dans les rapports. Je l'utilise pour enregistrer des informations sur l'ampleur des violations, les types de données compromises et les réponses apportées par les banques, notamment les mesures correctrices mises en œuvre après un incident.

5. Conformité réglementaire : Cette catégorie comprend les indications sur la manière dont les banques respectent les exigences légales et réglementaires en matière de protection des données. Cela inclut la mention de normes comme le RGPD (Règlement Général sur la Protection des Données) ou autres exigences spécifiques à l'institution.

L'utilisation de ce système de codage me permet de quantifier et d'analyser les occurrences de risques potentiels et de mesures proactives au sein des rapports. En documentant ces éléments de manière systématique, je suis en mesure d'identifier des tendances et de faire ressortir les bonnes pratiques en matière de protection des données, basées sur les résultats obtenus. Ce processus de

codage, réalisé manuellement, garantit également une rigueur d'analyse, en me permettant de porter une attention particulière aux nuances dans le langage utilisé dans les rapports.

En résumé, le processus de codage, effectué manuellement, m'a permis de structurer les informations de manière organisée. Cette approche facilite une analyse approfondie des rapports annuels des banques sur la gestion des risques liés à la protection des informations personnelles, tout en fournissant un cadre cohérent pour interpréter les données recueillies.

3.5 Analyse des Données

Dans le contexte de notre recherche portant sur la cybersécurité et la gestion des risques relatifs à la protection des renseignements personnels dans les banques canadiennes, nous avons conduit une analyse détaillée des divulgations concernant les risques liés à la sécurité des données personnelles pour chaque institution. L'objectif principal de cette analyse est d'évaluer la complétude de ces divulgations ainsi que leur conformité aux normes et réglementations en vigueur au Canada.

La littérature met en évidence l'importance considérable d'une divulgation proactive des risques pour instaurer la confiance des clients et des investisseurs, tout en atténuant l'incertitude relative à la sécurité des données. Selon Dainelli et al. (2013), une communication proactive d'informations pertinentes sert de signaux fiables, permettant aux parties prenantes de prendre des décisions éclairées. Cela s'inscrit parfaitement dans notre première question de recherche sur comment les banques canadiennes utilisent-elles la divulgation proactive des risques associés à la protection des renseignements personnels pour renforcer la confiance des clients et des investisseurs ? En explorant cette question, nous avons cherché à identifier dans quelle mesure les banques communiquent clairement sur les risques de cybersécurité et les mesures d'atténuation qu'elles mettent en place.

Les résultats de notre analyse ont été examinés sous l'angle du cadre conceptuel de risques, telle que présentée par Mun (2012), Hubbard et Seiersen (2023). Ainsi, nous avons analysé comment les banques abordent les enjeux de cybersécurité et de protection des données dans leurs divulgations, en réponse à notre seconde question de recherche à savoir quelles stratégies les banques canadiennes mettent-elles en œuvre pour identifier, évaluer et gérer les risques associés à la protection des renseignements personnels, et comment ces pratiques contribuent-elles à leur

résilience face aux cybermenaces? Pour répondre à cette question, nous avons identifié les éléments clés des divulgations, en évaluant leur profondeur, leur clarté et leur conformité avec les exigences réglementaires.

Cette approche qualitative a été orientée par un désir de comprendre comment les institutions financières gèrent les risques liés à la confidentialité des informations, tout en respectant les obligations légales et réglementaires. À travers l'analyse des tendances, des similitudes et des disparités dans les risques divulgués par les banques, nous avons tenté de dégager des enseignements significatifs, offrant ainsi une vision éclairante de leur gestion des questions de confidentialité et de cybersécurité.

En conclusion, l'analyse minutieuse des divulgations relatives aux risques de sécurité des données personnelles, réalisée dans le cadre de notre étude, a pour but d'éclairer les pratiques des banques en matière de communication et de gestion des risques. Les objectifs de notre recherche visent à renforcer les stratégies de gestion des risques et à améliorer les politiques de divulgation dans les banques canadiennes afin de garantir la protection des renseignements personnels. Grâce à une méthodologie axée sur l'analyse qualitative des rapports annuels des banques, nous pouvons identifier les bonnes pratiques à adopter et les domaines nécessitant des améliorations potentielles. Cette démarche contribue à enrichir la compréhension des interactions entre les banques et leurs parties prenantes dans le paysage financier canadien, tout en soulignant l'importance d'une gestion proactive des risques pour protéger les données sensibles des clients. Cette démarche contribue à enrichir la compréhension des interactions entre les banques et leurs parties prenantes dans le paysage financier canadien, tout en soulignant l'importance d'une gestion proactive des risques pour protéger les données sensibles des clients.

CHAPITRE 4

RÉSULTATS ET DISCUSSION

Ce chapitre rapporte les résultats obtenus à l'issue de notre recherche. Il est divisé en quatre grandes sections. La première répond à la question suivante : Les banques canadiennes recourent-elles à la divulgation proactive des risques liés à la protection des renseignements personnels dans leurs rapports annuels pour renforcer efficacement la confiance des clients et des investisseurs? Les deuxième et troisième sections du chapitre présentent le sommaire des résultats. La quatrième section décrit les mesures de sécurité mises en place par les banques pour protéger les données personnelles.

4.1 Sommaire des résultats

Il ressort de notre étude que les rapports annuels de chacune des trente-quatre banques étudiées comportent une section dédiée spécifiquement aux risques liés à la protection des renseignements personnels des clients. Toutes les banques ont donc évalué et rapporté les risques relatifs à la vie privée de leurs clients. L'analyse des rapports sociaux des grandes entreprises canadiennes réalisée par Serres et Gendron (2006) met en lumière certaines lacunes clés dans la manière dont ces entreprises abordent la gestion des risques, en particulier dans le secteur bancaire. Il est préoccupant de constater que, bien que les banques canadiennes aient commencé à intégrer de nouvelles exigences pour les clients et les fournisseurs dans leurs politiques de financement et d'appels d'offres, elles semblent traiter la gestion des risques de manière timide et peu dynamique. Cette approche minimaliste pourrait non seulement entraver leur capacité à anticiper et à atténuer efficacement les risques, mais également influencer négativement la confiance des parties prenantes dans leur engagement envers des pratiques de gouvernance responsables. Dans le cadre de notre étude, nous avons examiné comment les banques canadiennes abordent la présentation des risques associés à la protection des renseignements personnels ainsi que les stratégies qu'elles emploient pour gérer ces risques. Les résultats obtenus montrent que ces institutions adoptent des démarches proactives, lesquelles ont pour objectif, en théorie, de renforcer la confiance des clients et des investisseurs. Nous avons constaté que toutes les banques canadiennes ont effectivement abordé les risques dans leurs divulgations, indiquant ainsi une volonté claire de transparence. Cette

tendance à la transparence est essentielle dans le contexte actuel, où la protection des renseignements personnels est devenue une préoccupation majeure pour les clients et les investisseurs. Cela répond à notre première question de recherche sur comment les banques canadiennes font recours à la divulgation proactive des risques liés à la protection des renseignements personnels dans leurs rapports annuels pour renforcer efficacement la confiance des clients et des investisseurs. Nous pouvons également observer que ces institutions ne se contentent pas de déclarer simplement leur engagement envers la protection des données. Elles élaborent sur les types de risques identifiés, les mesures mises en œuvre pour atténuer ces risques, ainsi que les protocoles de réponse en cas de violation de données. Les banques canadiennes peuvent ainsi renforcer la confiance des clients et des investisseurs à plusieurs niveaux. D'abord, en divulguant de manière proactive les risques associés, elles montrent qu'elles prennent la sécurité des données au sérieux et qu'elles anticipent les préoccupations de leurs parties. Cette démarche proactive peut également atténuer les craintes des clients concernant les éventuels abus ou négligences dans la gestion de leurs informations personnelles. De plus, les rapports annuels offrent une plateforme pour détailler les investissements réalisés dans des technologies de sécurité avancées, tels que le chiffrement des données et les systèmes de détection des intrusions. En communiquant clairement ces efforts, les banques construisent une image de responsabilité et de diligence, ce qui est crucial pour fidéliser la clientèle. Enfin, la régularité et la consistance de ces divulgations jouent un rôle clé dans la perception de la fiabilité de l'institution. En communiquant régulièrement sur les évolutions réglementaires et les nouvelles menaces liées à la cybersécurité, les banques canadiennes non seulement renforcent la confiance, mais elles se positionnent également comme des leaders d'opinion dans le domaine de la sécurité des renseignements personnels. En somme, la divulgation proactive des risques associés à la protection des renseignements personnels représente un élément crucial dans la stratégie de communication des banques canadiennes. Cela leur permet non seulement de respecter les exigences réglementaires, mais également de forger des relations de confiance durable avec leurs clients et investisseurs.

En s'appuyant sur la théorie de la signalisation formulée par Dainelli et al. (2013), il apparaît que le partage d'informations pertinentes sur les risques permet aux banques de construire une image positive et de renforcer leur légitimité auprès de leurs parties prenantes. Cette transparence, qui est particulièrement accentuée dans la seconde section de notre chapitre où nous examinons les risques

divulgués par les trente-quatre banques, joue un rôle crucial dans la création d'un climat de confiance. La divulgation des risques identifiés ne se limite pas à une simple obligation réglementaire, mais représente un engagement proactif envers la gestion des renseignements personnels, reflétant ainsi la volonté des banques de se positionner comme des acteurs fiables dans le secteur financier.

Dans la troisième section, nous détaillons les mesures de sécurité que ces banques ont mises en place pour protéger les données personnelles. Cette approche est complémentaire à la divulgation des risques, car elle permet de démontrer concrètement les efforts déployés pour mitiger ces risques. En fournissant des détails sur les technologies de sécurité adoptées, les banques ne se contentent pas de déclarer leur engagement, mais elles montrent également qu'elles prennent au sérieux la responsabilité qui leur incombe. Ce lien entre la divulgation des risques et les mesures de sécurité renforce encore davantage la confiance des clients et des investisseurs, conformément aux principes de la théorie de la signalisation.

Par ailleurs, cette pratique des banques est en phase avec l'esprit de la Loi modernisant des dispositions législatives en matière de protection des renseignements personnels qui stipule que les organisations ont l'« obligation de réaliser une évaluation des facteurs relatifs à la vie privée dans certaines situations ». Ainsi, en respectant ces obligations légales et en communiquant de manière transparente sur les risques et les mesures de sécurité, les banques non seulement se conforment à la réglementation, mais elles établissent aussi des normes de confiance et de sécurité, contribuant ainsi à la solidité du paysage financier. L'analyse des divulgations effectuées par les banques canadiennes, en lien avec la théorie de la signalisation et les lois sur la protection des renseignements personnels, démontre que la transparence et la proactivité dans la gestion des risques sont essentielles pour renforcer la confiance des clients et des investisseurs. Ce chapitre illustre comment ces pratiques peuvent être intégrées dans une stratégie de communication globale, contribuant ainsi à la fidélisation de la clientèle et à la stabilisation du marché financier.

En outre, notre recherche aborde une question complémentaire : « Quelles sont les stratégies mises en œuvre par les banques canadiennes pour identifier, évaluer et gérer les risques associés à la protection des renseignements personnels, et comment ces pratiques leur permettent-elles de mieux faire face aux cybermenaces ? » En nous référant au cadre conceptuel des risques de Hubbard et Seiersen (2023), nos résultats révèlent que les banques adoptent des processus systématiques et

rigoureux pour gérer les risques. Elles mettent notamment l'accent sur la sensibilisation et la formation de leurs employés, conscient que le facteur humain est souvent la première ligne de défense contre les menaces cybernétiques. Les banques signalent également leur volonté d'investir dans des technologies avancées, ainsi que la nécessité d'effectuer des évaluations régulières des risques, afin de s'assurer que leurs pratiques en matière de sécurité sont actualisées face à l'évolution rapide des menaces numériques. Cela souligne l'importance d'une approche proactive et dynamique dans la gestion des risques.

Malgré ces efforts, il est crucial de souligner que les institutions continuent d'être exposées à des cyberattaques. Cette réalité soulève des interrogations quant à l'efficacité des mesures préventives adoptées et souligne la complexité croissante des menaces. En dépit de la mise en place de systèmes de sécurité, les banques doivent constamment évoluer et s'adapter aux nouvelles méthodes utilisées par des attaquants malveillants. Cela souligne la nécessité d'une culture de sécurité proactive, impliquant une mise à jour régulière des protocoles et des processus de gestion des risques.

Cette recherche contribue à améliorer les pratiques de gestion des risques au sein du secteur financier canadien. En identifiant les stratégies proactives déjà en place dans ces banques, notre étude vise à renforcer au sein des banques la sécurité des données et à protéger les informations personnelles des clients. Une meilleure appréhension des interactions entre la divulgation des risques et la confiance des parties prenantes peut également orienter les banques dans la création de stratégies plus efficaces pour construire leur réputation et améliorer leurs performances sur le marché.

En conclusion, nos résultats offrent des perspectives précieuses pour comprendre comment les banques canadiennes abordent la divulgation des risques et les défis associés à la protection des données personnelles. Ces découvertes peuvent constituer un outil essentiel, non seulement pour les institutions bancaires elles-mêmes, mais également pour les régulateurs et d'autres parties prenantes cherchant à renforcer la sécurité des données dans un environnement numérique en constante évolution. En renforçant les capacités des banques à faire face aux cybermenaces, nous garantissons non seulement la résilience des institutions financières, mais aussi la confiance du public envers l'ensemble du système bancaire.

Dans les sous-sections qui suivront, nous commencerons par examiner les risques liés à la protection des renseignements personnels tels qu'ils sont divulgués par les trente-quatre banques canadiennes étudiées. Cette section mettra en évidence les types de risques identifiés et les menaces potentielles qui pèsent sur les données personnelles des clients. Ensuite, nous aborderons les mesures de gestion du risque mises en place par ces banques, en analysant les stratégies et technologies adoptées pour protéger les informations personnelles ainsi que les protocoles de réponse en cas d'incidents. Cette structure nous permettra de comprendre de manière approfondie comment les banques naviguent dans le paysage de la protection des données et renforcent leur engagement envers la sécurité et la transparence.

4.2 Risques liés à la protection de renseignements personnels divulgués par les banques étudiées

Les trente-quatre banques étudiées ont rapporté divers types de risques liés à la protection de données personnelles. Le tableau 3 en annexe résume les risques liés à la protection de renseignements personnels divulgués par les trente-quatre banques étudiées pour la période allant de 2020 à 2022, ainsi que les procédures mises en place pour gérer ces risques (annexe2).

Avant d'aborder les risques identifiés, il est nécessaire de préciser le processus de formulation des catégories de risques. Nous avons établi neuf catégories liées à la protection des renseignements personnels, définies par une approche systématique d'extraction et d'analyse des informations issues des rapports annuels des banques canadiennes.

Nous avons classé les informations en lien avec les risques, leurs conséquences potentielles, ainsi que les procédures de gestion associées. Cette démarche de codage est conforme aux standards de la recherche qualitative, comme le soulignent Valéau et Gardody (2016), qui reconnaissent que le codage favorise une analyse structurée et rigoureuse.

Notre analyse approfondie des rapports a permis de mettre en lumière les mesures de sécurité spécifiques et les politiques visant à protéger les données personnelles, suivant le cadre proposé par Familoni et Shoetan (2024). Par ailleurs, un système d'analyse comparative a été utilisé pour rassembler et confronter les informations des différents rapports, facilitant ainsi l'identification des tendances et des disparités dans les pratiques des institutions financières. Les travaux de Thomas

et al. (2014) et de Pickvance (2001) soulignent que cette méthode comparative est cruciale pour identifier les meilleures pratiques et les éventuelles lacunes dans la gestion des risques.

4.2.1 Le risque lié au manque de connaissances concernant les mises à jour et les meilleures pratiques en matière de protection des renseignements personnels

La banque HSBC Canada, la banque Manuvie Canada, la banque de développement du Canada,les Alberta Treasury Branches et la banque Alterna ont signalé un risque lié à la méconnaissance des bonnes pratiques de protection des données personnelles. Ce risque découle de l'exposition cumulative aux violations de données. Comme le soulignent Solove et Schwartz (2011), il est crucial d'avoir une compréhension approfondie des lois et des pratiques de protection de la vie privée, ainsi que de rester informé des mises à jour et des évolutions en matière de protection des données personnelles. En négligeant les mises à jour importantes des logiciels et des systèmes, et les pratiques de sécurité recommandées, les individus et les organisations peuvent laisser des failles ouvertes dans leur système, ce qui peut être exploité par des cybercriminels pour accéder, voler ou compromettre des informations sensibles. Ces actions pourraient entraîner des conséquences graves telles que le vol d'identité, la fraude financière, la perte de données confidentielles et une atteinte à la réputation. Conformément à Ghernaouti (2016), il est essentiel pour toute entité de considérer la sécurité informatique de manière holistique et stratégique, en établissant une politique de sécurité claire, en sensibilisant et en formant ses employés, et en mettant en place des mesures préventives et correctives.

4.2.2 Le risque lié à la modification des lois et règlements ainsi que la complexité à interpréter certaines lois canadiennes

Les banques examinées dans cette étude, notamment la banque Scotia, la banque Royale du Canada, la banque Equitable (EQ) et Tangerine, sont confrontées à un risque substantiel lié aux changements réguliers des lois et règlements, combinés à la difficulté de l'interprétation de certaines lois canadiennes. La nature changeante du paysage juridique et réglementaire peut poser des défis significatifs en termes de conformité pour ces institutions financières. Il devient ardu tant pour les individus que pour les organisations de suivre et de comprendre ces évolutions. Ce manque de clarté peut entraîner des lacunes dans la prise en compte des lois pertinentes ou conduire à des interprétations erronées, exposant ainsi les banques concernées à des risques juridiques et financiers considérables. Hogg (2007) met en lumière les subtilités et les défis associés à

l'interprétation des lois canadiennes, en soulignant les répercussions potentielles des modifications législatives et réglementaires sur la gestion des risques juridiques. La non-conformité aux lois et règlements en vigueur peut engendrer diverses conséquences préjudiciables telles que des amendes, des litiges, des préjudices à la réputation et d'autres impacts néfastes. Il est impératif pour ces banques de demeurer vigilantes quant aux évolutions légales pertinentes. En cas de doute ou de complexité, la consultation d'experts juridiques qualifiés s'avère essentielle pour garantir la conformité et pour atténuer les risques associés à la complexité des lois et règlements.

4.2.3 Le risque lié à la sécurité de l'information

Les banques incluses dans cette étude, à savoir la banque Scotia, la banque Nationale, la banque de Montréal, la banque JP Morgan Canada et la CIBC, font face à un risque significatif lié à la sécurité de l'information. Ce risque implique la menace potentielle pour des données sensibles, confidentielles ou personnelles d'être compromises, volées, altérées ou détruites de manière non autorisée. Schneier (2001) corrobore que les menaces à la sécurité de l'information peuvent émaner de diverses origines, telles que des cybercriminels, des employés malveillants, des erreurs humaines, des défaillances techniques, voire des catastrophes naturelles. En l'absence de mesures de sécurité adéquates, les conséquences d'une violation de la sécurité de l'information peuvent s'avérer gravissimes. Il est impératif pour les individus et les organisations, notamment les banques, de mettre en place des politiques, des technologies et des pratiques de sécurité robustes pour protéger de manière efficace leurs informations. En prenant des mesures proactives pour renforcer la sécurité de l'information, les banques peuvent réduire les risques associés à la vulnérabilité de leurs données sensibles.

4.2.4 Le risque lié à la cybersécurité et aux technologies de l'information (TI) ainsi aux tiers

Les banques impliquées dans cette analyse, notamment banque HSBC Canada, Revolut, EQ Bank, banque Canadienne Impériale de Commerce, Canada - Société Générale, Coast Capital Savings, la banque Scotia, la banque Laurentienne, la banque de Montréal (BMO), la banque JP Morgan Canada, Desjardins, la banque Toronto-Dominion Canada Trust (TD) et banque Comerica, sont confrontées à un risque majeur lié à la cybersécurité, aux technologies de l'information (TI) et aux tiers. Selon les recherches de Pompon (2016), un risque notable associé à la cybersécurité et aux technologies de l'information réside dans la dépendance envers des fournisseurs externes, des

partenaires commerciaux ou d'autres tiers pour des services critiques ou le stockage de données sensibles. Lorsqu'une organisation s'appuie sur des tiers pour des services liés à la cybersécurité ou aux technologies de l'information, elle expose potentiellement ses propres systèmes et données aux vulnérabilités liées à ces tiers. Il est essentiel pour les banques de prendre des mesures proactives pour évaluer et atténuer les risques associés à leur dépendance envers des tiers en matière de cybersécurité et de technologies de l'information. En renforçant la vigilance et en mettant en place des mécanismes de contrôle efficaces, les banques peuvent mieux protéger leurs actifs numériques et réduire les risques de compromission des données.

4.2.5 Le risque lié au perfectionnement et l'évolution constante des technologies et des stratégies d'attaque (cybersécurité)

La banque Desjardins, la banque du Canada et EQ Bank, font face à un risque crucial lié au perfectionnement et à l'évolution constante des technologies et des stratégies d'attaque dans le domaine de la cybersécurité. Ce risque englobe l'accroissement de la sophistication des attaques, dont se servent des organisations criminelles, des initiés malveillants, des pirates informatiques et d'autres entités internes ou externes. Selon Mitnick (2017), ces acteurs malveillants exploitent l'avancement technologique pour concevoir des attaques plus complexes et insaisissables, rendant ainsi leur détection et prévention plus ardues pour les systèmes de sécurité en place. Dans ce contexte en constante évolution, les entreprises sont confrontées à la nécessité impérieuse d'améliorer en permanence leurs mesures de sécurité pour contrer ces menaces en perpétuelle mutation. Il revient donc aux institutions financières de rester vigilantes et de constamment revoir et renforcer leurs dispositifs de sécurité pour être capable de faire face à ces nouveaux défis et protéger efficacement leurs systèmes et leurs données sensibles des attaques sophistiquées.

4.2.6 Le risque lié à la complexité des systèmes et des processus de collecte et de stockage des données

La banque Royale du Canada, l'EQ, la First Ontario, la Citi Canada et les Caisses Populaires Acadiennes sont confrontées à un risque significatif lié à la complexité croissante de leurs systèmes et processus de collecte et de stockage des données. Ce risque découle de la possibilité d'erreurs et de vulnérabilités accrues. Plus un système ou un processus est complexe, plus il devient difficile à maintenir et à sécuriser de manière efficace. Conformément aux observations de Perrow (1999), la complexité excessive des systèmes au sein d'une entreprise peut entraîner des failles de sécurité,

des incohérences dans les données, des conflits de gestion et des difficultés à assurer la conformité réglementaire. Il est impératif pour ces institutions financières de simplifier autant que possible leurs systèmes et processus de collecte et de stockage des données afin de réduire les risques associés à cette complexité. En rationalisant leurs opérations et en adoptant des approches plus simples et plus cohérentes, les banques peuvent renforcer leur sécurité et leur conformité tout en minimisant les risques liés à la gestion des données.

4.2.7 Le risque lié à la sécurité infonuagique

La banque de Montréal, cybersécurité, la banque JP Morgan Canada, les Services financiers Le choix du Président, la banque RFA du Canada, la banque Motus et les Caisses Populaires Acadiennes font face à un risque majeur en matière de sécurité infonuagique. Ce risque de sécurité associé au cloud, ou infonuagique, représente une menace potentielle pour la confidentialité, l'intégrité ou la disponibilité des données stockées dans le cloud, comme l'indique Schneier (2015). Ces risques englobent des vulnérabilités de sécurité, des attaques de piratage, des erreurs de configuration, des problèmes de conformité, voire des incidents de perte de données. Ainsi, il est impératif tant pour les fournisseurs de services cloud que pour les utilisateurs d'adopter des mesures de sécurité efficaces pour atténuer ces risques et assurer une protection adéquate des données sensibles. Il incombe aux institutions financières de mettre en place des politiques de sécurité robustes et des mécanismes de contrôle appropriés pour garantir la protection des données stockées dans le cloud. En renforçant la sensibilisation à la sécurité, en s'assurant de la conformité aux normes de sécurité et en procédant à des évaluations régulières des risques, ces banques peuvent réduire les probabilités d'incidents liés à la sécurité infonuagique et préserver la confiance de leurs clients.

4.2.8 La non-conformité aux lois et réglementations en matière de protection des renseignements personnels

La banque HSBC Canada, la banque du Canada, la banque Nationale du Canada, la banque Tangerine, la Coast Capital Savings, la banque Laurentienne, la banque Toronto-Dominion Canada Trust (TD) et Banque Comerica font face à un risque critique lié à la non-conformité aux lois et réglementations en matière de protection des renseignements personnels. Ce risque de non-conformité se traduit par une menace pour une organisation qui ne respecte pas ses obligations

légales relatives à la collecte, au traitement et à la protection des données personnelles, comme le souligne Cavoukian (2009). Cela peut inclure la non-conformité à la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) au Canada, le non-respect des dispositions du Règlement général sur la protection des données (RGPD) en Europe, de la *California Consumer Privacy Act* (CCPA) en Californie, ou d'autres lois sur la confidentialité des données qui régissent la collecte et l'utilisation des informations personnelles des individus. Il est impératif pour ces banques de mettre en place des politiques et des pratiques rigoureuses pour garantir la conformité aux lois et réglementations en matière de protection des renseignements personnels. En veillant à la transparence dans la collecte de données, en mettant en œuvre des pratiques de consentement appropriées et en adoptant des mesures de sécurité robustes, ces institutions peuvent réduire les risques de non-conformité et renforcer la confiance de leurs clients en matière de confidentialité des données.

4.2.9 Le risque lié à la dépendance envers la technologie et des tiers

La Canadian Western Bank, la General Bank of Canada, la banque Peoples du Canada et Les Alberta Treasury Branches font face à un risque critique lié à leur dépendance envers la technologie et des tiers. Ce risque implique la vulnérabilité potentielle d'une organisation aux perturbations ou défaillances associées à l'utilisation de technologies externes ou de prestataires de services tiers. Il peut survenir dans des situations où une entreprise repose fortement sur des logiciels, des infrastructures cloud ou d'autres technologies fournies par des tiers. Selon les avertissements de Stross (2007), la dépendance croissante envers la technologie et les systèmes informatiques expose les organisations à des risques accrus de cybercriminalité et de vulnérabilités liées aux tiers. Ainsi, il est essentiel pour ces banques de mettre en place des plans de continuité informatique, de contractualiser de manière solide avec les fournisseurs de services et d'effectuer des évaluations régulières de la sécurité et de la fiabilité des technologies utilisées. La mise en œuvre de ces mesures proactives permettra à ces institutions financières de renforcer leur résilience face aux risques liés à la dépendance envers la technologie et des tiers, assurant ainsi une continuité opérationnelle et une protection accrue des données sensibles.

4.3 Les mesures de gestion du risque lié à la protection des renseignements personnels mise en place par les trente-quatre banques canadiennes étudiées.

Tel que mentionné dans le tableau 3, les trente-quatre banques étudiées ont mis en place diverses procédures pour gérer les risques liés à la protection des renseignements personnels pour la période allant de 2020 à 2022.

4.3.1 Banque Laurentienne

Cette banque a mis en place essentiellement trois mesures. En premier lieu, elle maintient une surveillance constante de son réseau informatique pour détecter toute activité suspecte, les tentatives d'intrusion ou les cybermenaces émergentes. Cette mesure permet une détection précoce des menaces et une réponse rapide en cas d'incident.

En deuxième lieu, la banque Laurentienne a investi dans des technologies et des pratiques de cybersécurité avancées pour renforcer ses défenses contre les cyberattaques. Cela inclut l'utilisation de pare-feu avancés, de programmes de détection d'intrusion et de cryptage des données sensibles pour assurer la sécurité et l'intégrité de son réseau.

En troisième lieu, la banque Laurentienne organise des programmes de formation réguliers pour sensibiliser son personnel aux bonnes pratiques de sécurité informatique, aux techniques de phishing, aux signaux d'alerte des cyberattaques, ainsi qu'aux mesures à prendre en cas d'incident de cybersécurité.

4.3.2 Banque Nationale

Cette banque a instauré principalement quatre mesures. Premièrement, la banque Nationale a mis en place un cadre de gestion des risques non financiers reposant sur trois lignes de défense. Ce cadre implique les services opérationnels et transversaux chargés de détecter, évaluer et traiter les risques au premier niveau. Au deuxième niveau, il existe un contrôle spécialisé dans la gestion des risques non financiers, intégré dans un département supervisant ce cadre de gestion des risques.

Deuxièmement, renforcement de la cybersécurité et de la continuité des activités. La Banque Nationale améliore ses règles de sécurité et mène des campagnes de sensibilisation pour prévenir les cybermenaces telles que le phishing et le ransomware. Une politique de protection des informations a été révisée, mettant l'accent sur la conformité au Règlement général sur la protection des données (RGPD) et la manipulation de données sensibles en dehors du lieu de travail.

Troisièmement, sensibilisation du personnel à la sécurité informatique. Dans le but de renforcer les connaissances en matière de cybersécurité au sein de toute l'organisation, la Banque Nationale a étendu un programme de sensibilisation en ligne à l'ensemble de son personnel. Ce programme s'échelonnera sur une période de quatre ans afin d'assurer une formation approfondie et continue pour garantir la sécurité des systèmes d'information et la protection des données sensibles de la banque. Cette initiative vise à sensibiliser les employés aux risques cybernétiques et à promouvoir de bonnes pratiques en matière de sécurité informatique à tous les niveaux de l'entreprise.

Quatrièmement, Collaboration avec des partenaires et utilisation d'équipes spécialisées en cybersécurité. La Banque Nationale s'engage à renforcer la sécurité de ses systèmes et de ses informations en collaborant étroitement avec des partenaires pour réduire les risques liés à la technologie. Elle utilise des équipes spécialisées en cybersécurité pour adapter son programme interne et mettre en place une structure de gouvernance basée sur une gestion saine des risques technologiques, y compris les cyberrisques, la cybercriminalité et la protection des renseignements personnels.

4.3.3 La Banque Impériale de Commerce du Canada (CIBC)

Cette banque a adopté essentiellement cinq dispositifs. Premièrement, investissement accru dans les mécanismes de défense en cybersécurité. La banque CIBC a récemment décidé d'investir davantage de ressources dans le renforcement de ses systèmes de sécurité afin de lutter contre les cybermenaces croissantes. Cette décision s'accompagne de la mise en place de mesures de protection avancées visant à renforcer la résilience de la banque face aux menaces cybernétiques actuelles. En allouant des ressources supplémentaires à la sécurité informatique, la CIBC démontre son engagement à protéger les données de ses clients, à assurer la confidentialité des informations sensibles et à maintenir la confiance de ses parties prenantes en matière de sécurité numérique.

Deuxièmement, mise en place d'examens du risque stratégique, d'outils technologiques et de programmes de sécurité de l'information. Dans le cadre de ses efforts pour renforcer sa posture de sécurité, la banque CIBC a mis en place des examens du risque stratégique, des outils technologiques avancés et des programmes dédiés à la sécurité de l'information. Ces initiatives ont pour objectif d'évaluer de manière proactive les risques, de mettre en place des mesures d'atténuation efficaces, d'exploiter des technologies de pointe pour renforcer la résilience du système de sécurité et de développer des programmes complets visant à protéger les informations sensibles de l'organisation.

Troisièmement, surveillance constante des cybermenaces mondiales et des exigences réglementaires. Dans le cadre de ses pratiques de gestion des risques, la banque CIBC maintient une surveillance continue sur les cybermenaces à l'échelle mondiale ainsi que sur les exigences réglementaires en constante évolution. Cette vigilance accrue permet à la CIBC d'améliorer en permanence ses contrôles internes et ses processus de protection des systèmes informatiques. En restant à l'affût des menaces émergentes et des évolutions réglementaires, la banque ajuste ses stratégies de cybersécurité, renforce sa résilience face aux attaques potentielles et se conforme aux normes et directives en vigueur pour assurer la sécurité de ses données et la confidentialité de ses clients.

Quatrièmement, exercices de cybersécurité, protocoles d'intervention et assurance contre les cyberrisques. Afin de renforcer sa posture en matière de cybersécurité, la banque CIBC organise des exercices réguliers de simulation de cyberattaques, a établi des protocoles d'intervention détaillés pour faire face aux incidents de cybersécurité et a pris une assurance contre les risques liés à la cybercriminalité pour atténuer les éventuelles pertes en cas d'attaque. Ces mesures proactives visent à améliorer la préparation de la banque face aux menaces numériques en simulant des scénarios réalistes, en garantissant une réponse rapide et efficace en cas d'incident, et en réduisant les conséquences financières potentielles à la suite d'une cyberattaque.

Cinquièmement, évaluation périodique de l'assurance, surveillance continue des risques et améliorations constantes des stratégies de sécurité. La banque CIBC procède régulièrement à l'évaluation de ses dispositifs d'assurance contre les cybermenaces, maintient une surveillance constante des risques émergents et effectue des améliorations continues de ses stratégies de sécurité

informatique. Cette approche globale vise à minimiser les répercussions potentielles des cyberincidents en s'assurant que les protections et les mesures de sécurité sont à jour et efficaces. En évaluant et en adaptant constamment ses pratiques en matière de cybersécurité, la CIBC s'efforce de rester en avance sur les menaces numériques, de renforcer sa posture de sécurité et de garantir la protection des données sensibles de ses clients.

4.3.4 La Banque Desjardins

Cette banque a établi surtout cinq actions. D'abord, allouer des fonds pour la création d'un laboratoire de cybersécurité. Desjardins a investi un montant de 845 000 $ pour le financement de la création d'un laboratoire dédié à la cybersécurité et à la protection des données personnelles. Cette initiative vise à renforcer les capacités internes de l'entreprise pour faire face aux menaces croissantes liées à la cybersécurité. Les fonds alloués sont principalement utilisés pour le recrutement de professionnels hautement qualifiés dans ces domaines critiques, permettant ainsi à Desjardins de bénéficier de l'expertise et des compétences nécessaires pour prévenir et contrer les cyberattaques, assurant ainsi la sécurité des informations sensibles de ses clients.

Suivant cela, suivi et conformité aux réglementations en matière de cybersécurité. Afin de garantir la conformité aux réglementations en constante évolution en matière de cybersécurité, Desjardins effectue un suivi étroit des développements des exigences réglementaires, même au niveau provincial. Conscient de l'importance de se conformer aux normes et aux lois en vigueur pour assurer la protection des données sensibles, le Mouvement Desjardins se tient prêt à répondre aux exigences du projet de loi C-26. Ce projet de loi vise à renforcer la cybersécurité des systèmes de télécommunication et des cybersystèmes essentiels, y compris les systèmes bancaires du secteur privé sous réglementation fédérale. En anticipant et en se préparant activement aux nouvelles réglementations, Desjardins démontre son engagement envers la sécurité des informations et la protection des données de ses membres, tout en assurant la conformité avec les normes de cybersécurité en vigueur.

En troisième lieu, Mise en place d'une gouvernance solide en matière de cybersécurité. Desjardins a nommé des professionnels chevronnés tels que Dominique Jodoin et Sonia Corriveau au sein de son conseil d'administration pour instaurer une gouvernance solide en matière de cybersécurité.

Ces experts possèdent des compétences approfondies en technologies de l'information et en cybersécurité, et apportent leur expertise pour renforcer les mesures de prévention contre la cybercriminalité au sein de l'organisation. Grâce à la présence de ces membres qualifiés au conseil, Desjardins bénéficie d'une direction éclairée et proactive en matière de cybersécurité, assurant ainsi une gestion efficiente des risques liés à la sécurité informatique et la protection des données sensibles des membres.

En quatrième position, programmes de modernisation de renforcement de sécurité. Desjardins s'engage dans des programmes de modernisation visant à renforcer la sécurité de ses environnements critiques. Ces initiatives ont pour objectif de prévenir les perturbations, d'améliorer les contrôles de sécurité, de gérer les menaces provenant à la fois de sources internes et externes, et de mener des analyses par scénarios ainsi que des suivis opérationnels pour identifier et gérer de manière proactive les risques. Grâce à ces programmes de modernisation, Desjardins démontre son engagement à maintenir des standards élevés en matière de sécurité et de gestion des risques, tout en assurant la confidentialité et l'intégrité des données de ses membres et parties prenantes.

Et enfin, au cinquième point, bureau de la sécurité Desjardins. Desjardins a mis en place un bureau de la Sécurité qui pour mission spécifique de garantir la protection des membres, des clients et de leurs informations personnelles. Ce bureau est chargé de mettre en place des mesures de sécurité adaptées pour prévenir et contrer les cyberincidents potentiels. En accordant une attention particulière à la sécurité des données et à la confidentialité des informations sensibles, le bureau de la sécurité joue un rôle essentiel dans la protection des membres et clients de Desjardins contre les menaces numériques. En surveillant de près les tendances en matière de cybersécurité et en mettant en œuvre des protocoles de sécurité robustes, ce bureau contribue à renforcer la résilience de l'organisation face aux cyberattaques et à assurer un environnement sûr et sécurisé pour les interactions financières et les activités des membres et clients de Desjardins.

4.3.5 La Banque du Canada

Cette banque a mis en œuvre quatre mesures clés. En premier lieu, investissements dans les technologies et les processus informatiques. La Banque du Canada a pris des mesures significatives

en allouant des ressources stratégiques pour améliorer ses technologies et ses processus informatiques. Cette initiative vise à renforcer la posture de sécurité de l'institution financière et à réduire les impacts potentiels des cyberattaques et des incidents de sécurité. La Banque du Canada investi dans des technologies de pointe et optimise ses processus informatiques afin de démontrer son engagement à préserver l'intégrité de ses opérations, à protéger les données sensibles qu'elle détient et à garantir la confiance du public dans la sécurité de ses systèmes.

En deuxième lieu, test de la capacité de réponse aux cyberattaques et de reprise des activités. La banque du Canada a mis en œuvre des exercices internes de test et de simulation afin d'assurer sa préparation face aux cyberattaques et sa capacité à reprendre rapidement ses activités après un incident. Ces exercices visent à évaluer la réactivité de la banque en cas de cyberincident et à identifier les mesures nécessaires pour garantir une reprise efficiente des opérations. La Banque du Canada a pu grâce à ces tests mettre en lumière ses points forts et identifier les domaines nécessitant des améliorations afin de renforcer sa résilience face aux cybermenaces.

En troisième lieu, collaboration avec des partenaires externes. La banque du Canada a initié une collaboration fructueuse avec des partenaires externes pour évaluer la résilience du système financier canadien. Des exercices conjoints ont été mis en place pour évaluer la capacité du système financier à faire face à d'éventuelles menaces et perturbations. Cette collaboration intersectorielle permet de rassembler différentes expertises et perspectives, renforçant ainsi la compréhension des défis en matière de sécurité financière et contribuant à l'amélioration continue de la résilience du système. En travaillant de concert avec des acteurs clés du secteur, la Banque du Canada favorise une approche collaborative visant à renforcer la sécurité globale du système financier canadien, assurant ainsi sa stabilité et sa protection face aux risques émergent.

En quatrième lieu finalement, recrutement et fidélisation d'employés qualifiés et diversifiés dans le domaine de la cybercriminalité. La Banque du Canada met en avant le recrutement et la fidélisation d'une main-d'œuvre diversifiée et hautement qualifiée dans le domaine de la cybersécurité pour renforcer ses capacités de prévention contre la cybercriminalité. Elle met l'accent sur la diversité et l'excellence professionnelle et vise à constituer une équipe solide et polyvalente capable de faire face aux défis croissants de la sécurité informatique. La Banque du Canada recrute des talents variés et en favorisant un environnement inclusif. Elle renforce sa

position pour anticiper, détecter et contrer les menaces cybernétiques de manière proactive. Cette démarche démontre son engagement à rester à la pointe des technologies et des pratiques de sécurité, tout en favorisant un environnement de travail diversifié et inclusif pour ses employés.

4.3.6 La Banque BMO

Cette banque a instauré principalement trois mesures. En premier lieu, investissements dans l'Unité Crime financier et l'infrastructure technologique. BMO effectue des investissements significatifs dans son unité de lutte contre la criminalité financière ainsi que dans son infrastructure technologique pour renforcer les capacités de ses équipes dans la détection et la prévention des menaces en cybersécurité. Ces investissements sont déployés à l'échelle internationale, couvrant les régions de l'Amérique du Nord, de l'Europe et de l'Asie, dans le but d'assurer la sécurité des données de ses clients et de ses employés à travers le monde. En renforçant son unité de lutte contre la criminalité financière, BMO s'engage à identifier, enquêter et lutter contre les activités malveillantes qui menacent la sécurité financière de ses parties prenantes. Parallèlement, en améliorant son infrastructure technologique, BMO vise à mettre en place des outils et des systèmes avancés pour prévenir les cyberattaques et protéger les informations confidentielles. Ces initiatives soulignent l'engagement de BMO envers la sécurité des données et la protection de la vie privée de ses clients à l'échelle mondiale.

En deuxième lieu, améliorations continues des capacités technologiques. Avec l'évolution rapide des services bancaires numériques, BMO poursuit ses investissements dans des améliorations innovantes de ses capacités technologiques pour répondre aux attentes croissantes de ses clients et garantir la sécurité de leurs données. En se concentrant sur l'innovation technologique continue, BMO s'efforce d'offrir des services numériques performants et sécurisés, reflétant ainsi son engagement envers l'excellence opérationnelle et la protection des informations sensibles de ses clients. En investissant dans des technologies de pointe, BMO cherche à rester à la pointe des évolutions du secteur bancaire numérique, assurant ainsi une expérience client optimisée et sécurisée. Ces améliorations constantes de ses capacités technologiques témoignent de sa vision stratégique pour se positionner en tant que leader dans le domaine des services bancaires numériques tout en offrant un environnement sûr et fiable pour ses clients.

En troisième lieu, innovation technologique et utilisation des données avancées et de l'intelligence artificielle. BMO s'est engagé dans des initiatives technologiques novatrices en se concentrant sur l'utilisation avancée des données et de l'intelligence artificielle. En investissant dans des solutions telles que la gestion de données avancées, les outils analytiques sophistiqués et l'intelligence artificielle, BMO cherche à transformer fondamentalement la manière dont elle opère et dont elle offre ses services à sa clientèle. Cette approche proactive a pour objectif d'améliorer ses capacités de détection, de prévention et de réponse face aux cyberincidents, renforçant ainsi sa posture de sécurité et sa résilience face aux menaces numériques.

4.3.7 La Banque TD Canada Trust

Cette banque a introduit principalement quatre mesures. Avant tout, la banque TD accorde une importance capitale à la surveillance, à la gestion et à l'amélioration constante de sa posture en matière de cybersécurité. En adoptant une approche proactive, la banque met en place des programmes à l'échelle de l'entreprise conformes aux normes de gestion des cybermenaces de l'industrie. Cette démarche vise à atténuer les risques liés à la technologie et à la cybersécurité, ce qui permet une détection rapide et une résolution efficace des incidents. Grâce à cet engagement continu envers la sécurité numérique, la Banque TD renforce sa capacité à protéger les données sensibles de ses clients et à maintenir la confiance dans ses services financiers.

En second plan, au sein de la banque TD, un sous-comité dédié à la cybersécurité a été mis en place, regroupant des membres de la haute direction. Ce comité a pour mission de superviser de manière proactive et de fournir des directives essentielles sur la gestion des risques en matière de cybersécurité. Il se concentre notamment sur la surveillance et la réponse aux cybermenaces telles que le cyberterrorisme, la cyberfraude et le cyberespionnage. Grâce à l'expertise et à l'engagement de ce sous-comité, la Banque renforce sa capacité à anticiper, prévenir et contrer les menaces numériques, assurant ainsi la protection des actifs et des informations sensibles de l'organisation.

Pour le troisième point, la banque TD a établi un solide cadre de gestion du risque opérationnel et a mis en œuvre des programmes dédiés à la technologie et à la cybersécurité. Ces initiatives incluent des tests de résilience pour évaluer la capacité de l'organisation à faire face à des situations critiques, des processus de gestion des changements visant à assurer la robustesse des systèmes et des

pratiques de gestion des actifs informationnels pour garantir leur intégrité et leur valeur. En mettant l'accent sur la préservation des actifs et la protection des informations sensibles, ces efforts soutiennent les objectifs commerciaux de la Banque TD tout en renforçant sa posture en matière de sécurité et de confidentialité des données.

Concernant le quatrième point, la banque TD a instauré un bureau dédié à la gouvernance des données d'entreprise pour développer et appliquer des normes et des pratiques cohérentes à l'échelle de l'organisation concernant la création, l'utilisation et la conservation des actifs informationnels. Ce bureau veille à prévenir toute pratique inappropriée ou qui pourrait compromettre la sécurité des données et l'intégrité de l'image de la Banque. En mettant l'accent sur la transparence, la conformité réglementaire et la protection des informations, ce bureau joue un rôle essentiel dans la promotion d'une culture de gestion des données responsable, renforçant ainsi la confiance des clients et des parties prenantes dans les pratiques de gouvernance des données de la Banque.

4.3.8 La Banque Scotia

Cette banque a déployé fondamentalement quatre initiatives. Premièrement, la banque Scotia met en œuvre des mesures proactives pour surveiller et gérer les risques associés aux cyberincidents en réalisant des investissements stratégiques dans la technologie, en renforçant l'expertise interne et en souscrivant des assurances pour atténuer les pertes potentielles. En se focalisant sur l'innovation technologique, elle vise à améliorer sa posture de sécurité et sa capacité à réagir efficacement aux menaces numériques. Par le développement continu de l'expertise interne en matière de cybersécurité, la Banque s'assure d'avoir les ressources nécessaires pour anticiper, identifier et contrer les cyberattaques. De plus, en obtenant des assurances spécifiques contre les risques liés à la cybercriminalité, la Banque se prémunit contre les conséquences financières potentielles d'éventuels incidents. Ces investissements multiples soulignent l'engagement de la Banque Scotia à maintenir un environnement sécurisé pour ses opérations et à protéger les intérêts de ses clients et partenaires.

Deuxièmement, la banque Scotia accorde une importance particulière au renforcement de son processus d'évaluation et de surveillance des risques associés aux fournisseurs tiers. Cette initiative

se concentre sur l'amélioration de la gouvernance des tiers, l'optimisation du processus de sélection des fournisseurs et l'adoption de technologies plus robustes pour gérer de manière efficace les risques inhérents aux tiers. En renforçant sa gouvernance des tiers, la Banque Scotia vise à garantir la conformité réglementaire, la sécurité des données et la continuité des opérations. En améliorant son processus de sélection des fournisseurs, elle cherche à évaluer avec soin les partenariats externes afin de réduire les vulnérabilités et les risques. En intégrant des technologies avancées pour surveiller et gérer les risques liés aux tiers, la Banque Scotia renforce sa capacité à anticiper, évaluer et atténuer les menaces provenant de son écosystème de fournisseurs externes. Cette approche proactive souligne l'engagement de la Banque à assurer la sécurité et la fiabilité de ses opérations avec ses partenaires commerciaux.

Troisièmement, mise en place d'un comité de gestion du risque et d'une équipe de gestion des risques. La Banque Scotia a institué un comité de gestion des risques chargé de valider le cadre de gestion des données et la politique de gouvernance en place. Parallèlement, une équipe dédiée à la gestion des risques surveille de façon proactive les données et l'utilisation de l'intelligence artificielle pour détecter et gérer efficacement les risques associés. Le comité de gestion des risques joue un rôle essentiel dans la validation et l'amélioration continue du cadre de gestion des données, garantissant ainsi sa conformité aux normes et aux politiques internes. Quant à l'équipe de gestion des risques, son rôle consiste à surveiller activement les différentes sources de données et les applications d'intelligence artificielle pour identifier et atténuer les risques. Grâce à cette approche intégrée entre le comité de gestion des risques et l'équipe dédiée, la Banque Scotia renforce sa capacité à prévenir les incidents liés aux données et à maintenir un environnement sécurisé pour ses activités et ses interactions avec les clients.

Quatrièmement, la banque Scotia adopte une approche collaborative en matière de gestion des risques liés aux données, en mettant l'accent sur la prévention des risques financiers, réglementaires et de réputation. Elle favorise la collaboration étroite avec l'ensemble des parties prenantes, internes et externes et cherche à établir un environnement de travail synergique et transparent pour relever les défis liés à la cybersécurité et à la protection des données. En impliquant activement toutes les parties prenantes dans le processus de gestion des risques, la Banque Scotia s'assure d'avoir une vision globale et inclusive des enjeux, ce qui favorise une meilleure identification, évaluation et atténuation des risques. Cette approche collaborative

renforce la culture de la sécurité des données au sein de l'organisation et renforce la confiance de ses clients et de ses partenaires en matière de protection des données sensibles.

4.3.9 La Banque Alterna

Cette banque a fixé essentiellement quatre orientations. Pour commencer, Alterna a pris l'engagement ferme de protéger les données de ses sociétaires en adoptant une approche proactive en matière de cybersécurité. Cette approche comprend une planification stratégique avant-gardiste, qui anticipe les évolutions technologiques et les menaces potentielles, ainsi qu'un investissement constant dans les dernières technologies de sécurité. En outre, la banque met l'accent sur l'amélioration continue de ses contrôles de sécurité, garantissant ainsi une protection renforcée des informations confidentielles de ses membres. En privilégiant l'innovation et la vigilance, Alterna démontre son engagement envers la confidentialité et la sécurité des données, tout en offrant une expérience bancaire fiable et sécurisée à ses sociétaires.

Comme deuxième point, amélioration constante des capacités de défense. Alterna a entrepris des mesures significatives pour renforcer ses capacités de défense en cybersécurité. Cette initiative englobe une amélioration continue de la qualité des contrôles de sécurité et une augmentation de la préparation à réagir efficacement aux attaques cybernétiques. En investissant dans des technologies de pointe et en mettant l'accent sur la formation du personnel, la banque s'efforce d'assurer une protection accrue des données de ses clients. Grâce à ces efforts constants d'amélioration, Alterna se positionne en tant qu'institution financière proactive et résiliente, prête à faire face aux défis actuels et futurs en matière de cybersécurité.

En troisième instance, la banque Alterna maintient son engagement envers la sensibilisation à la cybersécurité en offrant une formation continue à ses employés. Cette formation vise à renforcer la conscience des risques liés à la cybersécurité et à garantir la résilience des technologies de l'entreprise. En outre, Alterna participe activement à l'échange d'informations sur les menaces et les risques avec d'autres institutions financières, favorisant ainsi la collaboration sectorielle en matière de sécurité. En partageant les meilleures pratiques et en restant informée des tendances émergentes, la banque renforce ses défenses contre les cybermenaces et contribue à renforcer la sécurité de l'écosystème financier dans son ensemble.

Au quatrième rang, l'équipe cybernétique d'Alterna s'investit pleinement dans la fourniture de conseils et d'astuces précieux aux sociétaires afin de les aider à renforcer leur sécurité lorsqu'ils utilisent les services bancaires en ligne. Ces conseils incluent des pratiques recommandées en matière de cybersécurité, des informations sur la protection des identifiants et des transactions en ligne, ainsi que des astuces pour reconnaître et éviter les tentatives de phishing et d'autres formes d'escroqueries numériques. En partageant activement ces connaissances avec les clients, Alterna vise à autonomiser les sociétaires dans la protection de leurs comptes et de leurs données personnelles, renforçant ainsi la confiance dans l'utilisation des services bancaires en ligne de la banque.

4.3.10 La Banque Comerica

Cette banque a lancé quatre mesures fondamentales. Pour commencer, la banque Comerica accorde une attention particulière à la gestion des risques liés à la cybersécurité et à l'information, consciente des impacts potentiels sur sa réputation. Pour contrer efficacement ces risques, la banque met en œuvre des mesures de protection robustes visant à prévenir les cyberattaques et les fraudes. Ces mesures incluent des stratégies de sécurité avancées, des protocoles de surveillance proactifs et des contrôles de sécurité rigoureux pour garantir la confidentialité, l'intégrité et la disponibilité des informations sensibles. En adoptant une approche proactive et en investissant dans des technologies de pointe, la banque Comerica renforce sa posture de sécurité et assure la confiance de ses clients dans la protection de leurs données et de leurs transactions financières.

Comme deuxième point, la banque Comerica accorde une importance primordiale à la maintenance et à la sécurisation de ses systèmes informatiques essentiels, couvrant notamment les systèmes d'autorisation de transaction, de compensation et de règlement, ainsi que ses centres de données critiques. En mettant en place des processus rigoureux de gestion des risques et de sécurité, la banque s'efforce de garantir la fiabilité et l'intégrité de ses infrastructures technologiques. Des mesures proactives sont prises pour prévenir les interruptions de service potentielles causées par des défaillances techniques, des cyberattaques, des pannes de courant ou d'autres incidents imprévus. En investissant dans la surveillance continue, les mises à jour de sécurité et les tests de résilience, la banque Comerica démontre son engagement envers la disponibilité et la protection de

ses systèmes informatiques critiques, assurant ainsi des services bancaires fiables et sûrs à ses clients.

En troisième instance, adaptation au travail à distance. Face à l'essor du travail à distance entraîné par la pandémie, la banque Comerica Canada prend des mesures proactives pour adapter ses practices de sécurité afin de protéger ses opérations contre les risques accrus associés à cette nouvelle façon de travailler. La banque reconnaît l'importance de renforcer ses protocoles et mesures de sécurité pour garantir la protection des données sensibles et prévenir d'éventuelles cybermenaces. En mettant l'accent sur la sensibilisation des employés, le renforcement de l'authentification multi-facteurs et la surveillance accrue des activités en ligne, la banque Comerica s'efforce d'assurer la continuité des activités tout en maintenant un niveau élevé de sécurité informatique. Cette approche proactive souligne l'engagement de la banque à s'adapter aux nouvelles réalités du travail à distance tout en protégeant les intérêts de ses clients et de ses opérations.

Et enfin au quatrième rang, gestion des conséquences des incidents. En cas d'incidents affectant l'accès en ligne aux services bancaires ou aux informations de compte, la banque Comerica dispose de plans d'action prêts à être déployés rapidement pour atténuer les conséquences sur ses opérations. La banque s'engage à réagir de manière efficace afin de limiter les impacts sur ses clients, à maintenir leur confiance et à respecter les exigences réglementaires en vigueur. En mettant en œuvre des processus de gestion d'incident bien définis, en assurant une communication transparente avec les parties prenantes et en mettant l'accent sur la résolution rapide des problèmes, la banque Comerica démontre sa capacité à gérer de manière proactive les situations critiques et à garantir la continuité de ses services même en cas d'incident.

4.3.11 La Banque JP Morgan Canada

Cette banque a élaboré trois mesures essentielles. D'abord, la banque JP Morgan Canada accorde une importance capitale à la gestion des risques opérationnels, reconnaissant que tout écart dans les processus, la technologie ou les actions des individus peut compromettre la réalisation des objectifs de l'organisation. Pour atténuer ces risques, la banque a mis en place une série complète de programmes de gestion des risques opérationnels. Ces programmes couvrent un large éventail

de domaines, incluant les risques liés aux personnes, les risques criminels tels que la fraude et le blanchiment d'argent, les risques physiques, la sécurité de l'information, la continuité des opérations, ainsi que les risques associés aux sous-traitants et aux fournisseurs. En adoptant une approche holistique de la gestion des risques, La banque JP Morgan Canada s'efforce de prévenir, d'identifier et de gérer efficacement toute menace potentielle pesant sur ses opérations, assurant ainsi la sécurité, la stabilité et la conformité de ses activités.

Suivant cela, Système de gestion des risques opérationnels. La banque JP Morgan Canada maintient un cadre de gestion des risques opérationnels qui intègre les différents programmes de gestion des risques opérationnels. Ce cadre aide la banque à équilibrer efficacement le risque accepté dans ses opérations quotidiennes tout en cherchant à fournir des solutions à valeur ajoutée pour ses membres.

En troisième lieu, la banque JP Morgan Canada accorde une attention particulière à la protection de ses activités contre les cyberincidents, même si cette information n'est pas explicitement détaillée dans le texte initial. Il est implicite que la banque met en place des stratégies spécifiques pour gérer les risques liés à la sécurité de l'information et aux cyberincidents. Ces mesures incluses la mise en œuvre de contrôles de sécurité des données robustes, l'élaboration de plans de continuité des activités pour faire face aux incidents, la fourniture de formations en cybersécurité pour sensibiliser et renforcer les compétences du personnel, ainsi que la mise en place de procédures de gestion des incidents pour réagir rapidement et efficacement en cas d'attaques. En adoptant une approche proactive et en investissant dans les meilleures pratiques en matière de cybersécurité, la banque JP Morgan Canada s'engage à protéger la confidentialité, l'intégrité et la disponibilité de ses données, assurant ainsi la résilience de ses activités face aux menaces numériques actuelles et émergentes.

4.3.12 La Banque HSBC Canada

Cette banque a déployé fondamentalement quatre initiatives. Premièrement, HSBC consacre des ressources considérables à des investissements massifs dans des contrôles de sécurité à la fois commerciaux et techniques. Cette démarche vise à améliorer la prévention, la détection et l'atténuation des menaces liées à la cybersécurité, renforçant ainsi la protection des données tant

de l’organisation que de sa clientèle. Grâce à ces investissements stratégiques, HSBC s’engage pleinement à maintenir des normes élevées en matière de sécurité informatique, assurant la confidentialité et l’intégrité des informations.

Deuxièmement, HSBC mène une évaluation continue du paysage des menaces, en analysant de manière constante le niveau de risque des différentes formes d’attaques les plus répandues et en évaluant leurs impacts potentiels. Cette vigilance permanente permet à la banque d’anticiper les menaces émergentes et d’adapter ses stratégies de sécurité en conséquence. En surveillant de près les évolutions du domaine de la cybersécurité et en restant proactif dans sa réponse aux menaces, HSBC renforce sa posture de sécurité, réduisant ainsi les risques et protégeant efficacement ses systèmes et données sensibles.

Troisièmement, HSBC a mis en place une série complète de politiques et de systèmes de gestion visant à garantir des pratiques organisationnelles exemplaires, tout en assurant une surveillance et un contrôle efficaces de ses opérations. Grâce à ces politiques et systèmes robustes, la banque renforce la protection de ses données et renforce sa résilience face aux cyberincidents. En adoptant des normes élevées en matière de gouvernance et de conformité, HSBC démontre son engagement envers la sécurité des informations et la bonne gestion des risques, assurant ainsi la fiabilité et la sécurité de ses activités bancaires pour ses clients et partenaires.

Quatrièmement, HSBC accorde une grande importance à la sensibilisation et à la formation de son personnel en ce qui concerne la prévention des cybermenaces. La banque reconnaît le rôle crucial que jouent les employés dans la protection contre les attaques informatiques. C’est pourquoi elle s’engage à fournir à ses collaborateurs les outils nécessaires et les formations adéquates pour prévenir, atténuer et signaler les incidents de cybersécurité. En sensibilisant activement ses équipes et en les formant aux meilleures pratiques de sécurité informatique, HSBC renforce la posture de sécurité de l’organisation et contribue à maintenir la confidentialité et l’intégrité des données de l’entreprise et de sa clientèle. Cette démarche proactive démontre l’engagement de HSBC envers une culture de cybersécurité solide et protection des informations sensibles.

4.3.13 La Banque Royale du Canada

Cette banque a adopté essentiellement quatre dispositifs. En premier lieu, La banque Royale du Canada s'attaque au risque associé à l'utilisation, la possession, l'exploitation et l'adoption de systèmes informatiques pouvant entraîner des interruptions d'activité, des perturbations des services aux clients et des pertes de données confidentielles, pouvant entrainer des pertes financières, des atteintes à la réputation et des sanctions réglementaires. Une équipe mondiale d'experts en gestion des risques liés aux technologies de l'information surveille ces risques conformément au cadre de gestion du risque opérationnel de la banque.

En deuxième lieu, la banque Royale du Canada gère le risque lié à la cybersécurité, impliquant la perturbation ou l'interruption des opérations, ou la perte de données en raison d'une cyberattaque. Elle compte sur une équipe dédiée de professionnels spécialisés en technologie et en cybersécurité pour mettre en place un programme complet visant à protéger l'organisation des violations et autres incidents en veillant à la mise en place de contrôles de sécurité et d'exploitation adéquats.

En troisième lieu, renforcement du cadre de gestion du risque lié à la cybersécurité. La banque Royale du Canada améliore continuellement son cadre de gestion du risque lié à la cybersécurité pour accroître sa résilience et ses capacités en matière de cybersécurité. Cela comprend une surveillance en continu, l'analyse de renseignements sur les menaces, et le signalement d'événements et d'incidents suspects. Des investissements sont réalisés dans le programme de cybersécurité, et des scénarios, évaluations et simulations sont menés pour tester la stratégie de résilience de la banque.

En quatrième lieu, la Banque Royale du Canada aborde le risque lié à la gestion des informations, qui se réfère à l'incapacité à gérer de manière adéquate les données tout au long de leur cycle de vie, en raison de processus, de contrôles ou de technologies inadéquats. Pour atténuer ce risque, la banque a investi considérablement dans son équipe de chef des données de l'entreprise, ainsi que dans les unités fonctionnelles et régionales de gestion et de gouvernance des données. Cet investissement vise à sensibiliser le personnel aux risques liés à la gestion des informations et à améliorer la gestion de ces risques.

Enfin cinquième lieu, gestion du risque lié à la confidentialité. La confidentialité des données est une autre préoccupation majeure pour la Banque Royale du Canada. Le risque de confidentialité se concentre sur la possibilité que les données soient créées, collectées, utilisées, partagées, stockées ou détruites de manière inappropriée. Avec l'accent mis sur les solutions numériques et l'expansion des activités commerciales, la collecte, l'utilisation, le partage, la gestion et la gouvernance des données jouent un rôle crucial. Banque Royale du Canada travaille avec ses chefs des données et de la confidentialité pour continuer de mettre en place des normes et des pratiques organisationnelles qui définissent comment les données doivent être utilisées, protégées, gérées et régies de manière appropriée.

4.3.14 La Banque Revolut

Cette banque a mis en œuvre quatre mesures clés. Premièrement, gestion des cybermenaces. Revolut, en tant que prestataire de services financiers axé sur les applications, reconnaît les cybermenaces comme un risque majeur pour la sécurité des systèmes et des données de ses clients. La banque fait face à la gestion d'importantes quantités de données personnelles et confidentielles, et doit se conformer à des réglementations strictes en matière de protection et de confidentialité des données. Pour atténuer ces risques, Revolut a mis en place des pratiques de sécurité avancées, combinant des techniques et des contrôles organisationnels robustes pour renforcer la sécurité de ses systèmes d'information. En investissant dans des technologies de pointe, en sensibilisant et formant son personnel, et en surveillant en permanence les évolutions des menaces cybernétiques, Revolut démontre son engagement à protéger les informations de ses clients et à garantir un environnement financier sécurisé et fiable pour tous ses utilisateurs.

Deuxièmement, sécurité avancée des données et des systèmes. Revolut a mis en place des mesures telles que des tests de sécurité des applications, la gestion des vulnérabilités, des programmes de formation en entreprise sur la cybersécurité et les attaques par phishing, une protection avancée contre les menaces des points d'accès, des renseignements sur les menaces extérieures, une surveillance en temps réel de son infrastructure clé, une couverture de réponse aux incidents 24h/24 et 7j/7, des tests réguliers de tiers et des audits externes.

Enfin troisièmement, résilience opérationnelle. Revolut met l'accent sur la résilience opérationnelle pour gérer efficacement la disponibilité, les risques de continuité et la réponse aux perturbations opérationnelles. En cas de perturbations, qu'elles soient liées à des pannes technologiques, des cyberattaques ou d'autres incidents externes, maintenir la résilience opérationnelle aide à protéger les clients et à atteindre les objectifs de croissance. Revolut exploite un cadre de résilience opérationnelle qui définit les politiques, les procédures et la gouvernance pour surveiller et gérer la résilience des services commerciaux les plus importants pour les clients.

4.3.15 Coast Capital

Cette banque a établi surtout quatre actions. En premier, Coast Capital reconnaît l'importance cruciale d'évaluer la sécurité de ses fournisseurs tiers afin de garantir qu'ils respectent rigoureusement les normes et les pratiques essentielles en matière de cybersécurité. Cette démarche proactive permet de réduire au minimum les risques associés à la collaboration avec des partenaires externes. En menant régulièrement ces évaluations approfondies, Coast Capital renforce sa posture de sécurité et s'assure de la protection de ses données sensibles et de celles de ses clients.

En seconde position, Coast Capital accorde une attention soutenue à la surveillance continue de ses fournisseurs clés afin d'identifier, évaluer et atténuer les risques, qu'ils soient inhérents ou résiduels. Cette pratique rigoureuse englobe la création et le maintien d'un environnement de contrôle périodique, garantissant ainsi un niveau de sécurité optimal. Grâce à cette surveillance proactive et régulière, Coast Capital se positionne de manière proactive pour faire face aux menaces émergentes et assurer la fiabilité de ses opérations commerciales.

Par la suite, Coast Capital reconnaît l'impératif de rester constamment vigilant et de s'adapter en permanence en matière de gestion des risques informatiques et de cybersécurité afin de demeurer résilient face à la rapide évolution du paysage de la cybercriminalité. Cette démarche nécessite de prendre en considération la portée, la taille et la complexité de ses activités opérationnelles, ainsi que l'intégration croissante de technologies émergentes. En s'engageant dans une adaptation continue, Coast Capital se positionne de manière proactive pour anticiper les menaces émergentes, renforcer ses défenses et garantir la protection de ses actifs numériques et de la confidentialité de ses clients.

Enfin quatrième position, Coast Capital accorde une importance primordiale à la conformité réglementaire en tenant compte des nouvelles réglementations ou mises à jour relatives à la cybersécurité, à la protection des données et aux technologies émergentes. Pour rester en conformité, l'organisation s'adapter constamment aux exigences en évolution, ce qui requiert des ajustements continus dans ses pratiques et ses stratégies opérationnelles. Ces efforts supplémentaires visent à atténuer les impacts potentiels sur les opérations tout en renforçant la posture de conformité de Coast Capital et en préservant la confiance de ses parties prenantes.

4.3.16 Tangerine

Cette banque a introduit principalement quatre mesures. Pour commencer, Tangerine met en garde contre la potentielle menace posée par les offres de logiciels en ligne gratuits, qui pourraient être compromis par des logiciels malveillants. Afin de prévenir les risques de sécurité, il est fortement recommandé de ne télécharger des logiciels que depuis des sources fiables et des entreprises légitimes. En adoptant une approche de prudence et de vérification constante, les utilisateurs peuvent réduire significativement le risque d'infection par des logiciels malveillants et protéger la sécurité de leurs appareils et de leurs données sensibles.

En seconde lieu, Tangerine insiste sur l'impératif de maintenir la sécurité des mots de passe et des NIP en évitant de les partager avec quiconque. Il est vivement conseillé d'opter pour des mots de passe robustes, complexes et uniques, tout en veillant à ne pas les baser sur des informations personnelles faciles à deviner. En adoptant des pratiques de sécurité renforcées pour la gestion des mots de passe, les utilisateurs peuvent protéger efficacement leurs comptes et leurs données sensibles contre les tentatives de piratage et renforcer ainsi leur cybersécurité personnelle.

Pour le troisième point, Tangerine intègre un processus d'authentification des achats en ligne pour valider l'authenticité des transactions réalisées avec ses cartes, en envoyant un code de sécurité à usage unique par message texte. Cette procédure de vérification à deux facteurs ajoute une couche de sécurité supplémentaire en renforçant la protection des comptes contre les activités frauduleuses et les tentatives de cybercriminalité. En mettant en place cette mesure de sécurité efficace, Tangerine offre une tranquillité d'esprit accrue à ses clients tout en garantissant l'intégrité et la confidentialité de leurs transactions en ligne.

Au quatrième rang, protection de l'identité. Tangerine conseille d'être prudent face aux demandes de renseignements personnels et de contacter l'organisme par un autre canal officiel en cas de doute. Il est recommandé de s'inscrire à un service de surveillance du dossier de crédit et d'examiner régulièrement ses relevés bancaires pour repérer toute activité suspecte et informer immédiatement l'institution financière en cas de besoin.

4.3.17 FirstOntario

Cette banque a lancé quatre mesures fondamentales. Premièrement, la FirstOntario met en garde contre les dangers liés à la divulgation d'informations en ligne. Il est fortement recommandé d'éviter d'envoyer des données personnelles sensibles via des courriers électroniques ou des messages instantanés et de limiter la quantité d'informations personnelles divulguées en ligne pour diminuer les risques de vol d'identité et de piratage. En adoptant une approche de prudence et de confidentialité dans la gestion des informations en ligne, les individus peuvent renforcer leur sécurité numérique et protéger leur vie privée contre les menaces en ligne croissantes.

Deuxièmement, la FirstOntario recommande fortement d'adopter des pratiques de sécurité robustes en utilisant des mots de passe uniques, complexes et solides, tout en évitant de les réutiliser d'un compte à l'autre. La banque conseille qu'il est également essentiel de garder strictement confidentiel son code d'accès personnel (PAC) et de ne jamais le partager, que ce soit par message vocal, courriel ou téléphone. En suivant ces recommandations, les individus peuvent renforcer la sécurité de leurs comptes en ligne, réduire le risque de compromission de leurs informations personnelles et prévenir les potentielles tentatives d'accès non autorisé à leurs comptes et données sensibles.

Troisièmement, la FirstOntario met l'accent sur l'importance de sensibiliser ses clients aux dangers du phishing, une pratique où des acteurs malveillants se font passer pour des entités légitimes afin d'obtenir des informations confidentielles. La banque recommande vivement de rester vigilant et de ne pas ouvrir de pièces jointes, télécharger des logiciels ou cliquer sur des liens provenant de courriels ou de messages instantanés suspects. En adoptant une approche de prudence et en étant attentif aux signaux d'alerte du phishing, les clients de FirstOntario peuvent réduire les risques de

divulgation de leurs données personnelles et protéger leur identité et leurs comptes bancaires contre les attaques frauduleuses en ligne.

Quatrièmement, la FirstOntario préconise la pratique régulière de la vérification des relevés de compte et de carte de crédit, ainsi que la surveillance attentive du pointage de crédit des clients. La banque recommande d'activer les alertes sur les comptes en ligne afin d'être immédiatement informé en cas d'activité suspecte ou inhabituelle. En adoptant ces mesures proactives de surveillance et en restant vigilant quant à l'activité de leurs comptes, les clients de la FirstOntario peuvent détecter rapidement toute anomalie financière, prévenir la fraude éventuelle et protéger leurs comptes et leur identité contre les menaces de sécurité en ligne.

Cinquièmement, signalement des fraudes. En cas de soupçons de compromission du mot de passe, de perte, de vol ou d'utilisation non autorisée du compte, la FirstOntario recommande vivement de prendre des mesures immédiates en contactant sans délai la *Credit Union* pour signaler la fraude. Agir promptement dans de telles situations permet de limiter les dommages potentiels, de bloquer toute activité frauduleuse et de protéger efficacement les avoirs et les informations financières des clients. En signalant rapidement toute fraude présumée, les clients de la FirstOntario bénéficient d'un soutien et d'une assistance rapides pour atténuer les risques et préserver la sécurité de leurs comptes contre les menaces de sécurité en ligne.

4.3.18 Banque EQ

Cette banque a mis en œuvre quatre mesures clés. En premier lieu, la banque EQ accorde une importance primordiale à la protection de tous les renseignements personnels recueillis dans le cadre de ses opérations. Une entente de confidentialité détaille de manière transparente et explicite la manière dont les informations personnelles sont collectées, utilisées, partagées et sécurisées. En garantissant la confidentialité et la sécurité des données personnelles de ses clients, Banque EQ renforce la confiance et la fiabilité de ses services, tout en respectant les normes et réglementations en matière de protection de la vie privée. Cette démarche démontre l'engagement de la banque à assurer la confidentialité et la protection des renseignements sensibles de ses clients à chaque étape de leur interaction.

Ensuite, la banque EQ prend la responsabilité de la gestion de tous les renseignements personnels en sa possession avec sérieux et transparence. Dans le cadre de cette responsabilité, un chef de la protection des renseignements personnels est désigné pour superviser de manière proactive le programme et les pratiques de confidentialité de la banque. Cette nomination démontre l'engagement de Banque EQ à placer la protection des données personnelles au cœur de ses préoccupations, en veillant à ce que des mesures appropriées soient en place pour garantir la sécurité et la confidentialité des renseignements des clients. Grâce à cette approche proactive et responsable, la banque s'assure de respecter les attentes en matière de confidentialité et renforce la confiance de sa clientèle en matière de gestion et de protection des données personnelles.

En troisième position, la banque EQ a élaborée une entente en conformité avec la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE), démontrant ainsi son engagement à respecter les normes légales en vigueur en matière de confidentialité des données. Cette entente détaille de manière claire les types de renseignements personnels recueillis, leur utilisation, leur partage, ainsi que les mesures de sécurité mises en place pour garantir leur protection. De plus, elle précise les procédures concernant l'accès aux données, la communication en cas de questions sur la vie privée et les mécanismes permettant aux clients de contrôler leurs informations personnelles. En se conformant aux exigences légales établies par la LPRPDE, Banque EQ assure à ses clients que leurs informations personnelles sont gérées de manière responsable et conforme aux normes de confidentialité les plus rigoureuses.

Au quatrième point, la collecte de renseignements personnels par la banque EQ. Elle se fait de manière transparente et conforme aux pratiques de confidentialité en vigueur. Ces informations sont recueillies directement auprès des individus concernés, mais également de sources externes telles que des agences d'évaluation du crédit, des institutions financières et autres partenaires légitimes. Cette approche de collecte diversifiée vise à garantir l'exactitude et la pertinence des informations recueillies, dans le respect des normes de protection des données et de la vie privée. En ayant recours à des sources fiables et en mettant en place des protocoles de sécurité stricts, Banque EQ s'assure de la légitimité et de l'intégrité des renseignements personnels collectés, renforçant ainsi la confiance et la transparence dans sa gestion des données clients.

Enfin au cinquième point, la banque EQ utilise les renseignements personnels collectés de manière variée et spécifiée dans le cadre des services et des interactions avec les clients. Ces données sont essentielles pour mener des vérifications d'identité, évaluer la solvabilité lors de demandes de crédit, traiter les demandes de produits et services financiers, assurer une communication efficace avec les clients, gérer les risques associés aux opérations bancaires, prévenir la fraude, répondre aux obligations légales et réglementaires en vigueur, et bien d'autres aspects pertinents. En respectant les finalités explicites pour lesquelles les renseignements sont collectés, Banque EQ démontre son engagement à garantir la confidentialité des données de ses clients tout en fournissant des services personnalisés et sécurisés en accord avec les normes de protection des renseignements personnels.

4.3.19 Banque Manuvie Canada

Cette banque a mis en place une stratégie de gestion des risques liés à la technologie et à la sécurité informatique. La banque Manuvie Canada a pris des mesures proactives en établissant une fonction dédiée à la gestion des risques liés à la technologie pour réduire l'exposition aux risques liés à l'information. Sous la supervision du directeur de la sécurité de l'information, la banque a mis en place un programme complet de sécurité informatique visant à atténuer les risques liés à la sécurité des informations sensibles. Ce programme intègre un solide cadre de gestion de l'information et de cybersécurité, comprenant des politiques et des normes robustes ainsi que des contrôles appropriés pour protéger efficacement l'information et les systèmes informatiques contre les menaces. En outre, la banque propose des formations régulières de sensibilisation à la sécurité de l'information à l'ensemble de ses employés, renforçant ainsi la culture de la sécurité au sein de l'organisation et garantissant une vigilance constante face aux risques en matière de technologie et cybersécurité.

4.3.20 Services financiers Le choix du Président

Cette banque a déployé fondamentalement six initiatives. Premièrement, la formation des collègues sur la sécurité informatique. Elle est un processus essentiel qui vise à doter les employés des connaissances et des compétences nécessaires pour comprendre les meilleures pratiques en matière de sécurité, les risques liés à la cybercriminalité et les mesures à prendre pour protéger efficacement les données sensibles de l'entreprise. En fournissant une formation adéquate et adaptée, les

employés sont mieux préparés à reconnaître et à faire face aux menaces de sécurité, à contribuer et à renforcer la posture de sécurité de l'organisation et à prévenir les incidents de sécurité qui pourraient compromettre la confidentialité et l'intégrité des données de l'entreprise. Ce processus continu de sensibilisation à la sécurité garantit que les employés restent informés et engagés dans la protection des informations critiques de l'organisation.

Deuxièmement, les Services financiers Le choix du Président met en œuvre des contrôles et des tests réguliers pour garantir la sécurité des systèmes informatiques. Cette procédure implique l'établissement de mécanismes de surveillance et de vérification continus visant à détecter les vulnérabilités et les failles de sécurité potentielles. En effectuant des tests de sécurité réguliers, l'organisation identifie activement les points faibles de ses systèmes et met en place des mesures correctives pour renforcer sa résilience face aux menaces. Ces pratiques proactives permettent d'assurer un niveau optimal de sécurité informatique, de prévenir les incidents de sécurité et de protéger efficacement les données sensibles de l'entreprise contre les cyberattaques et les intrusions malveillantes.

Troisièmement, les Services financiers Le choix du Président met en place une pratique de maintenance des systèmes de protection des données qui revêt une importance capitale pour assurer une sécurité informatique optimale. Cette pratique implique la mise à jour régulière et la maintenance des systèmes de sécurité afin de garantir leur efficacité contre les menaces constamment évolutives. Cela comprend l'installation opportune de correctifs de sécurité, la mise à jour des logiciels antivirus et la surveillance proactive des activités suspectes. En veillant à ce que les systèmes de protection des données soient constamment optimisés et à jour, Services financiers Le choix du Président renforce sa capacité à prévenir les cyberattaques, à détecter rapidement les incidents de sécurité et à protéger de manière proactive les informations sensibles contre toute forme de compromission ou de violation de données.

Quatrièmement, les plans de gestion des cyberincidents qui détaillent les mesures à suivre en cas de perturbation majeure des opérations de l'entreprise due à une attaque informatique. Ces mesures comprennent la mise en place de procédures de sauvegarde des données robustes, la restauration rapide des systèmes touchés, ainsi que la communication efficace avec les parties prenantes pour limiter les impacts sur l'activité globale de l'entreprise. En mettant en œuvre ces plans, l'entreprise

se préparer à réagir de manière coordonnée et efficace face aux cybermenaces, réduisant ainsi les risques et minimisant les dommages causés par de telles situations critiques.

Cinquièmement, les Services financiers Le choix du Président présidé par le Président qui joue un rôle crucial dans l'allocation des ressources financières et techniques nécessaires à la mise en œuvre de mesures de sécurité avancées. Ces mesures visent à réduire les risques associés aux cyberattaques et à renforcer la posture de sécurité globale de l'entreprise. En investissant dans des technologies et des stratégies de sécurité de pointe, Services financiers Le choix du Président contribue à protéger les actifs de l'entreprise, à garantir la confidentialité des données sensibles et à assurer la continuité des activités face aux menaces numériques en constante évolution. Grâce à cet engagement envers la sécurité, l'entreprise se positionne de manière proactive pour faire face aux défis de la cybersécurité et maintenir la confiance de ses parties prenantes.

Enfin sixième point, les procédures, protocoles et normes de sécurité définis pour les fournisseurs tiers de services. Ils jouent un rôle crucial dans la protection des données sensibles de l'entreprise. Ces lignes directrices établissent des exigences rigoureuses en matière de sécurité que les fournisseurs tiers doivent respecter lorsqu'ils traitent des informations confidentielles ou sensibles de l'entreprise. En imposant ces normes élevées, l'entreprise s'assure que ses partenaires externes maintiennent un niveau de sécurité adéquat, aligné sur ses propres standards de sécurité. Cela garantit la confidentialité, l'intégrité et la disponibilité des données, renforçant ainsi la confiance dans les relations avec les tiers fournisseurs de services et réduisant les risques liés à la gestion externalisée des informations stratégiques.

4.3.21 Canadian Western Bank

Cette banque a fixé essentiellement quatre orientations. En premier lieu, la Canadian Western Bank met en place la gestion du risque technologique qui est un processus essentiel pour identifier les points de défaillance potentiels et garantir la résilience des systèmes informatiques. Cette action de la banque implique la mise en place de contrôles intégrés, tels que la gestion de la configuration pour assurer la cohérence des paramètres système, la gestion des changements pour contrôler les modifications apportées aux infrastructures, la gestion des capacités pour anticiper et gérer la demande de ressources informatiques, ainsi que des programmes dédiés à la gestion de la sécurité

de l'information pour protéger les actifs numériques de manière proactive. En adoptant une approche holistique de la gestion du risque technologique, Canadian Western Bank renforce sa capacité à anticiper, prévenir et répondre aux menaces émergentes, garantissant ainsi la stabilité de ses opérations et la protection de ses données sensibles.

En second lieu, dans le cadre de la gestion du risque de cybersécurité à Canadian Western Bank, un focus est mis sur la conception et la mise en œuvre efficace de technologies, de processus et d'outils appropriés pour anticiper, détecter et contrer les menaces émergentes et évolutives. Cette action de la banque comprend la mise en place de mesures proactives pour renforcer la résilience du réseau informatique, la surveillance constante des activités suspectes pour une détection rapide des intrusions, et une réponse efficace en cas d'incident de sécurité. De plus, des tests d'intrusion réguliers et des exercices d'évaluation des contrôles, menés par des tierces parties indépendantes, permettent d'identifier les vulnérabilités potentielles et d'optimiser en permanence les systèmes de sécurité.

En troisième lieu, la Canadian Western Bank met en place la gestion du risque lié aux tiers. Cette gestion se repose sur l'utilisation d'un cadre dédié à l'identification, l'évaluation, la gestion et la surveillance centralisée des risques associés à l'externalisation et aux partenariats avec des tiers. Une attention particulière est accordée à l'évaluation de l'environnement de contrôle interne des fournisseurs de services, en particulier des prestataires de technologies. Ce processus permet d'assurer une évaluation approfondie des pratiques de sécurité et de conformité des tiers, ainsi que de garantir la protection des données sensibles de l'institution financière. En mettant en œuvre un tel cadre, Canadian Western Bank renforce sa capacité à anticiper et à atténuer les risques liés à sa chaîne d'approvisionnement et à ses relations avec des acteurs externes, assurant ainsi la fiabilité et la sécurité de ses opérations dans un environnement de plus en plus complexe et interconnecté.

Au quatrième point, dans le cadre de la gestion du risque lié aux données chez Canadian Western Bank, une approche collaborative et holistique est adoptée pour minimiser les risques liés à la réputation, aux réglementations et aux aspects financiers. Cela implique une gestion proactive des données à travers des processus continus d'amélioration, en mettant l'accent sur la correction des données, la surveillance de la qualité des informations et le renforcement des protocoles de support. En renforçant constamment ces processus et en investissant dans des outils technologiques avancés,

l'objectif de la banque est d'assurer l'intégrité, la disponibilité et la confidentialité des données tout au long de leur cycle de vie. En adoptant une approche rigoureuse de gestion des risques liés aux données, Canadian Western Bank limite non seulement les impacts négatifs potentiels, mais aussi renforcer la confiance des clients, des régulateurs et des autres parties prenantes envers la sécurité et la fiabilité de ses pratiques en matière de données.

4.3.22 Banque de développement du Canada

Cette banque a lancé quatre mesures fondamentales. Tout d'abord, la banque de développement du Canada reconnaît l'importance critique de la gestion efficace du risque technologique, en particulier face à l'évolution constante des menaces en matière de cybersécurité. La direction de la banque met en œuvre des mesures proactives et robustes pour préserver la sécurité de ses systèmes informatiques, de ses données sensibles et de son infrastructure technologique. Cela inclut la mise en place de technologies de pointe, de processus de surveillance continue, de politiques de sécurité strictes et de programmes de sensibilisation des employés pour renforcer la résilience de l'organisation face aux menaces numériques.

En deuxième lieu, la banque investit continuellement dans son infrastructure technologique pour protéger ses systèmes et les données de sa clientèle. Elle déploie des capacités de détection et d'intervention en cas d'incident en partenariat avec des entreprises spécialisées en sécurité. De plus, des programmes de sensibilisation des employés, des contrôles de systèmes et de réseau, ainsi que des tests indépendants réguliers sont réalisés pour renforcer la sécurité des données.

En troisième position, processus d'approvisionnement et d'octroi de contrats. Dans le domaine de l'approvisionnement et de la passation de contrats, la banque de développement du Canada applique des principes rigoureux pour garantir la transparence, l'équité et l'efficacité des processus impliqués, ainsi que la gestion adéquate des fournisseurs externes. Des programmes spécifiques de gestion des risques tiers sont mis en place pour évaluer et atténuer les risques associés à ces partenariats extérieurs. Un cadre de gouvernance solide et des processus de contrôle préalable sont en place afin de superviser de manière proactive l'évaluation des risques liés aux tiers. Grâce à cette approche proactive et structurée, la banque de développement du Canada renforce sa résilience face aux risques liés aux fournisseurs externes, garantit l'intégrité de ses opérations

d’approvisionnement et maintient des standards élevés en matière de gestion des risques contractuels.

Pour le quatrième point, dans le domaine des interventions et du plan de reprise après sinistre, la banque de développement du Canada met en place un programme de formation dédié pour améliorer la gestion des incidents, en mettant l’accent sur la formation des spécialistes en exploitation et en cybersécurité des technologies de l’information. Cette formation vise à renforcer les compétences nécessaires pour une réaction efficace face aux incidents technologiques. La banque gère de manière proactive les incidents liés aux technologies et déploie un plan de reprise après sinistre afin de minimiser les impacts sur ses opérations en cas de cyber incident majeur. En adoptant cette approche préventive et réactive, la Banque de développement du Canada renforce sa préparation face aux scénarios d’urgence, garantissant ainsi une continuité opérationnelle sans heurts et une capacité à faire face rapidement aux défis liés à la sécurité des technologies de l’information.

4.3.23 Citizens Bank of Canada

Cette banque a adopté essentiellement quatre dispositifs. En premier lieu, la Citizens Bank of Canada s’engage fermement à maintenir une approche de gestion des risques solide, intégrée et proactive pour faire face à tous les risques auxquels elle est confrontée dans la réalisation de ses objectifs commerciaux. Le conseil d’administration joue un rôle essentiel en déterminant l’appétit pour le risque, assurant ainsi une compréhension claire des niveaux de risque acceptables pour l’atteinte des objectifs stratégiques de la banque. Cette démarche stratégique vise à garantir que la gestion des risques est intégrée dans toutes les activités de l’organisation, permettant une prise de décision éclairée et une anticipation proactive des menaces potentielles.

Ensuite, gouvernance et surveillance des risques. Au sein de Citizens Bank of Canada, le Conseil d’administration délègue ses pouvoirs pour les activités de gestion des risques à plusieurs comités, parmi lesquels figure *l’Executive Risk Committee* présidé par le *Chief Risk Officer*. Ce comité essentiel est chargé de superviser de manière proactive les risques à l’échelle de l’entreprise, d’analyser le profil de risque global de la banque, et de confirmer que tous les risques sont correctement identifiés, évalués et atténués. En adoptant cette approche stratégique, Citizens Bank

of Canada renforce sa gouvernance et sa surveillance des risques, garantissant une gestion proactive des menaces potentielles et une prise de décision éclairée en matière de risques. Cette structure permet à la banque de maintenir un environnement opérationnel sain et stable, tout en assurant la protection des intérêts de ses clients, de ses actionnaires et de l'organisation dans son ensemble.

Pour le troisième point, la Citizens Bank of Canada, l'*Executive Risk Committee* est constitué de plusieurs comités spécialisés couvrant divers domaines de risque tels que la conformité, les risques opérationnels, les risques de modèles, la politique de crédit, la gestion de l'actif-passif, les initiatives commerciales, la conduite et l'éthique. Ces comités jouent un rôle crucial dans la supervision et l'évaluation des risques spécifiques à leurs domaines respectifs, garantissant une approche holistique de la gestion des risques au sein de la banque. En mettant en place ces comités spécialisés, Citizens Bank of Canada renforce sa capacité à identifier, évaluer et atténuer de manière proactive les risques associés à chaque aspect de ses activités, assurant ainsi une gestion prudente et effective des risques à tous les niveaux de l'organisation.

Au quatrième rang, la Citizens Bank of Canada fournit une transparence et une communication proactive en matière de gestion des risques à travers son rapport de gestion dirigé par la direction. Ce rapport détaillé offre un aperçu complet des pratiques de gouvernance des risques au sein de la banque, mettant en lumière les processus robustes établis pour l'identification, l'évaluation et l'atténuation des risques, notamment ceux liés à la cybersécurité et aux cyber incidents. En partageant ces informations clés, Citizens Bank of Canada démontre son engagement envers la transparence et la responsabilité envers ses parties prenantes, tout en fournissant une vision claire de sa gestion proactive des risques. Cela permet non seulement de renforcer la confiance des investisseurs, des régulateurs et du public envers la banque, mais aussi d'assurer une prise de décision éclairée et une préparation adéquate face aux défis actuels et futurs en matière de risques.

4.3.24 General Bank of Canada

Cette banque a mis en œuvre deux mesures clés. Premièrement, la General Bank of Canada reconnaît l'importance cruciale de son modèle des trois lignes de défense, sachant que sa structure repose fortement sur la technologie pour l'échange et le traitement des données. Les risques de crédit de la banque sont étroitement liés à l'efficacité de son infrastructure technologique et à la

robustesse de ses mesures de sécurité des données. Ainsi, toute lacune technologique ou violation de données pourrait potentiellement entraîner des perturbations opérationnelles et accroître le risque de crédit pour l'organisation. Pour atténuer ces risques et renforcer sa résilience, la General Bank of Canada met en œuvre le modèle des trois lignes de défense. Ce cadre de gouvernance des risques permet une répartition claire des responsabilités entre les différentes parties prenantes, assurant ainsi une gestion efficace des risques et des contrôles internes à tous les niveaux de l'entreprise. En suivant ce modèle éprouvé, la banque renforce sa capacité à anticiper, prévenir et gérer les risques, garantissant ainsi une protection adéquate de ses activités, de ses clients et de sa réputation dans un environnement de plus en plus numérique et complexe.

Deuxièmement, la General Bank of Canada reconnaît l'importance critique de la gestion des risques liés aux tiers, en particulier dans un modèle d'indirect où elle dépend de tiers pour l'octroi de prêts ou la réalisation de transactions. Les faiblesses en termes de santé financière ou de pratiques de gestion des risques de ces tiers peuvent avoir un impact significatif sur le risque de crédit global de la banque, ainsi que sur la confidentialité des données sensibles, y compris celles de ses clients. Afin d'atténuer ces risques, la banque a établi un programme de gestion des risques liés aux tiers, aligné sur les meilleures pratiques de l'industrie et en conformité avec les directives du Bureau du surintendant des institutions financières (BSIF). Ce programme comprend des processus rigoureux de diligence raisonnable sur les principales relations avec les tiers, garantissant que leurs pratiques de gestion des risques respectent les normes et les exigences de la banque en matière de sécurité et de conformité. En mettant en œuvre cette approche proactive, General Bank of Canada renforce sa capacité à identifier, évaluer et atténuer les risques associés à ses partenaires commerciaux externes, assurant ainsi la protection des intérêts de l'organisation et de ses clients.

4.3.25 Versa Bank

Versa Bank a établi des services dédiés à la cybersécurité et aux opérations de développement des technologies bancaires et financières en partenariat avec sa filiale en propriété exclusive, *DRT Cyber Inc*. Cette collaboration permet à la banque de renforcer sa posture de sécurité numérique et d'innover dans le secteur des services financiers. La direction de Versa Bank demeure engagée dans une évaluation continue des données et des informations pertinentes, réagissant de manière proactive aux avancées technologiques et aux évolutions du paysage des menaces. En intégrant ces

initiatives stratégiques, Versa Bank montre son engagement envers la protection des données sensibles, la mise en œuvre de technologies de pointe et l'adaptation constante aux défis du secteur financier. Cette vision proactive et axée sur la technologie positionne Versa Bank comme un acteur innovant et sécurisé dans le domaine bancaire et financier.

4.3.26 La Banque Peoples du Canada

Cette banque a fixé essentiellement trois orientations. Au premier point, la banque Peoples du Canada a introduit de nouvelles lignes directrices en matière de gestion des risques informatiques et des cyberrisques en 2022. Cette initiative souligne son engagement fermement ancré à renforcer les mesures de sécurité et à atténuer les risques associés aux cyberincidents dans le cadre de ses opérations bancaires. En adoptant ces nouvelles lignes directrices, la Banque Peoples du Canada démontre sa volonté de protéger efficacement ses activités et ses clients contre les menaces émergentes en matière de cybersécurité. Cette démarche proactive renforce la résilience de l'institution face aux cybermenaces et témoigne de son engagement constant envers une gestion des risques informatiques robuste et adaptée aux défis technologiques actuels.

Au second point, information et sensibilisation. La banque Peoples du Canada publie un bulletin hebdomadaire visant à sensibiliser les différentes parties prenantes de l'organisation aux questions réglementaires, juridiques et aux développements importants liés aux risques, y compris ceux liés aux modèles, aux tiers et aux cyberrisques. Cette communication régulière a pour objectif de maintenir le personnel informé des enjeux critiques et des meilleures pratiques en matière de gestion des risques. En diffusant ces informations de manière proactive, la banque renforce la sensibilisation de son effectif aux risques et leur implication dans les efforts de gestion des risques. Cette approche éducative contribue à créer une culture d'entreprise axée sur la sécurité et la conformité, renforçant ainsi la posture globale de la Banque Peoples du Canada face aux divers défis en matière de gouvernance des risques.

Au troisième point, la banque Peoples du Canada maintient un engagement dynamique au sein d'associations industrielles telles que l'Association des banques et des sociétés de fiducie, l'Association des banquiers canadiens, l'Organisation canadienne des fournisseurs de comptes prépayés et l'Association canadienne des entreprises de technologies de paiement. Cette

participation proactive permet à la banque de rester à l'avant-garde des tendances, des réglementations et des meilleures pratiques au sein du secteur financier, y compris en ce qui concerne la cybersécurité. En collaborant et en échangeant avec d'autres acteurs clés de l'industrie, la Banque Peoples renforce sa compréhension des défis et des opportunités du secteur, tout en favorisant le partage de connaissances et l'adoption des normes de sécurité élevées. Cette implication active au sein des associations industrielles souligne l'engagement de la banque à rester à la pointe de l'innovation et de la sécurité dans un environnement financier en constante évolution.

4.3.27 Banque RFA du Canada

La banque RFA du Canada a déployé un cadre de gestion des risques opérationnels (GRE) complet comprenant des stratégies bien définies pour gérer les risques, que ce soit par l'évitement, le transfert, l'acceptation ou l'atténuation à travers des contrôles appropriés. Ce cadre intègre plusieurs éléments clés, tels que des auto-évaluations des risques et des contrôles réguliers, l'évaluation des risques pour les nouvelles initiatives commerciales, la surveillance et le *reporting* des risques, les tests de contrôle, le *reporting* et l'analyse des incidents de risque, la mise en place de plans d'atténuation, les tests de résistance et l'analyse de scénarios, la diligence raisonnable envers les fournisseurs tiers, ainsi que le maintien d'une couverture d'assurance d'entreprise appropriée. En adoptant cette approche globale et proactive en matière de gestion des risques opérationnels, la banque RFA du Canada renforce sa capacité à anticiper, évaluer et atténuer les risques, garantissant ainsi la stabilité de ses opérations et la protection de ses intérêts à long terme.

4.3.28 Banque Motus

Cette banque a mis en œuvre quatre mesures majeures. Premièrement, la banque Motus accorde une importance primordiale à la réduction de la complexité de ses systèmes en priorisant la consolidation de ses infrastructures informatiques. Cette approche vise à améliorer l'expérience client et utilisateur en simplifiant les processus internes et en optimisant les performances des systèmes. En rationalisant ses technologies et en réduisant la fragmentation des systèmes, la banque renforce son agilité opérationnelle, réduit les coûts liés à la maintenance et améliore la sécurité globale de son environnement informatique. Cette démarche stratégique permet à la Banque Motus d'offrir des services bancaires plus efficaces et innovants, tout en restant résiliente face aux défis technologiques actuels et futurs.

Deuxièmement, la banque Motus face à la montée de la cybercriminalité accorde une grande importance à la protection des informations sensibles. Elle reconnaît que la sécurisation des données est essentielle pour prévenir les interruptions de services, préserver la confiance des clients et éviter des pertes financières conséquentes. En outre, la conformité aux réglementations strictes sur la protection des données personnelles est un élément clé de sa stratégie pour éviter les sanctions lourdes pouvant résulter de la négligence en matière de sécurité des données. En investissant dans des technologies de pointe, en mettant en place des protocoles de sécurité robustes et en sensibilisant son personnel aux bonnes pratiques en matière de sécurité informatique, la Banque Motus renforce sa posture de cybersécurité et protège de manière proactive les informations confidentielles de ses clients. Cette approche proactive et axée sur la conformité réglementaire souligne l'engagement de la Banque Motus envers la protection des données et la confidentialité des informations sensibles.

Troisièmement, la banque Motus continue d'investir dans des technologies de pointe afin de protéger et sécuriser pleinement ses systèmes informatiques, réduisant ainsi les risques pour renforcer sa résilience opérationnelle et préserver sa réputation. La numérisation constante de l'expérience client est un pilier central de cette stratégie, visant à répondre de manière proactive et efficace aux attentes en constante évolution de sa clientèle. En modernisant ses infrastructures technologiques, en intégrant des solutions de cybersécurité avancées et en adoptant des pratiques robustes de gestion des risques, la Banque Motus renforce sa capacité à faire face aux menaces numériques émergentes et à garantir la sécurité des données confidentielles de ses clients. Cette approche proactive en matière d'innovation technologique permet à la banque de maintenir un avantage concurrentiel, de renforcer la confiance des clients et de s'adapter aux exigences changeantes du paysage bancaire numérique.

Quatrièmement, la banque Motus renforce ses pratiques de sécurité informatique en assurant une surveillance et un suivi continus des profils de risques informatiques. Elle améliore constamment son cadre de gouvernance informatique et sa stratégie en matière de cybersécurité. La banque examine régulièrement les accords de niveau de service avec ses fournisseurs externes, réalise des examens et audits externes des contrôles informatiques pour garantir leur efficacité, renforce la protection des informations personnelles de ses clients, sensibilise de manière continue son personnel aux bonnes pratiques en cybersécurité et renforce sa capacité de réponse aux incidents

potentiels. En mettant en œuvre ces mesures proactives et en se concentrant sur l'amélioration continue de ses pratiques de sécurité informatique, la Banque Motus démontre son engagement envers la protection des données, la prévention des incidents de sécurité et la sécurisation de son infrastructure contre les menaces numériques en évolution constante.

4.3.29 Banque Rogers

Cette banque a introduit principalement six mesures. Premièrement, la direction de la banque Rogers a mis en place un programme robuste dédié à la sécurité de l'information et à la cybersécurité. Ce programme vise à assurer la protection des données sensibles, notamment les renseignements personnels des clients et du personnel de manière proactive. En mettant l'accent sur la prévention des menaces et des incidents de sécurité, Banque Rogers s'engage à maintenir des normes élevées pour garantir la confidentialité, l'intégrité et la disponibilité des informations.

Deuxièmement, formations de sensibilisation à la sécurité. Dans le cadre du programme de sécurité de l'information et de cybersécurité de la banque Rogers, des formations spécialisées sont régulièrement fournies au personnel. Ces sessions de formation visent à sensibiliser les employés aux meilleures pratiques de sécurité, ainsi qu'à renforcer la culture de la sécurité à tous les niveaux de l'entreprise. En mettant l'accent sur l'éducation continue en matière de sécurité, Banque Rogers s'efforce de garantir que chaque membre du personnel comprend et contribue activement à la protection des données sensibles et à la prévention des menaces informatiques.

Troisièmement, au sein de Banque Rogers, des politiques et des procédures de sécurité clairement définies guident les employés dans la protection des données sensibles et des informations confidentielles. Ces politiques internes strictes assurent la conformité aux normes de sécurité les plus élevées et détaillent les mesures spécifiques à suivre en cas de menaces ou d'incidents de sécurité. Banque Rogers renforce sa posture de sécurité, protégeant ainsi efficacement les renseignements personnels des clients et du personnel contre les risques.

Quatrièmement, la banque Rogers a établi des mécanismes de surveillance des risques liés à la cybersécurité pour détecter rapidement les menaces éventuelles. Ces mécanismes comprennent des outils de surveillance avancés, des analyses proactives et des alertes en temps réel pour garantir une détection précoce des incidents de sécurité. En plus de cela, des contrôles sont en place pour

atténuer ces risques identifiés, et des plans de réponse aux incidents ont été élaborés pour permettre une intervention rapide et efficace en cas de violation de la sécurité. Grâce à cette approche proactive de surveillance des risques, Banque Rogers renforce sa capacité à protéger les données sensibles et à maintenir un environnement sécurisé pour ses clients et son personnel.

Cinquièmement, la banque Rogers, dans sa démarche de renforcement de la cybersécurité a pris une mesure supplémentaire en souscrivant des assurances contre les dommages liés aux violations de la cybersécurité, aux intrusions et aux attaques ciblées contre ses systèmes. Cette assurance cybersécurité renforce la résilience de l'organisation en apportant une protection financière en cas d'incident majeur impactant la sécurité des données. En s'assurant de cette manière, Banque Rogers démontre son engagement à minimiser les risques liés à la cybersécurité et à maintenir la confiance de ses clients, en garantissant une réponse efficace et des mesures d'atténuation adéquates en cas de cyberattaques.

Sixièmement, confidentialité des données. Dans le contexte actuel où la confidentialité des données revêt une importance capitale, la banque Rogers accorde une priorité absolue à la protection des données personnelles de ses clients et de son personnel. Consciente de sa responsabilité en tant que gardienne de ces informations sensibles, l'entreprise met en œuvre des mesures de sécurité robustes pour garantir la confidentialité et l'intégrité des données à tout moment. En instaurant une culture de respect et de protection des données, Banque Rogers s'engage à respecter les normes les plus strictes de confidentialité et à maintenir la confiance de ses parties prenantes en veillant à la sécurité et à la confidentialité des informations personnelles qu'elle détient.

4.3.30 Capital One

Cette banque a adopté essentiellement quatre dispositifs. Au premier point, la Capital One a mis en place un solide programme de gestion des risques opérationnels, supervisé par le responsable du risque opérationnel. Ce programme a pour objectif d'évaluer de manière approfondie le profil de risque opérationnel de l'entreprise et de mettre en œuvre des processus de contrôle essentiels pour atténuer les risques identifiés. Ces risques incluent, entre autres, la fraude, les menaces cybernétiques et technologiques, la gouvernance des données, les risques liés aux modèles, la gestion des fournisseurs et la continuité des activités. En se concentrant sur ces domaines critiques,

Capital One s'engage à garantir une gestion efficace des risques opérationnels, à renforcer sa résilience face aux menaces potentielles et à assurer la protection des actifs et des données de l'entreprise.

Au second point, la Capital One a mis en œuvre un système robuste de gouvernance, de gestion des risques et de conformité pour surveiller et gérer de manière proactive les risques, les contrôles, les problèmes et les incidents associés à chaque catégorie de risques. Ce système intégré offre la capacité d'enregistrer, d'analyser, d'agréger et de générer des rapports détaillés sur les risques dans toutes leurs dimensions. En utilisant cette approche globale, Capital One peut identifier précocement les risques émergents, évaluer l'impact sur l'ensemble de l'organisation et prendre des mesures correctives appropriées pour atténuer les risques. Capital One renforce sa capacité à assurer une gouvernance solide, à garantir la conformité et à maintenir la résilience opérationnelle face aux défis contemporains en matière de risques.

Au troisième point, la Capital One, dans le cadre de sa gestion des risques opérationnels a déployé des politiques, des normes, des processus et des contrôles rigoureux pour encadrer efficacement la gestion des risques opérationnels. Ces directives établissent un cadre clair et structuré pour identifier, évaluer et traiter les risques opérationnels de manière proactive. En mettant en place ces mesures, Capital One vise à offrir des expériences client de qualité tout en atteignant ses objectifs commerciaux de manière contrôlée et impartiale. En intégrant des pratiques solides de gestion des risques opérationnels dans l'ensemble de ses activités, l'entreprise renforce sa capacité à anticiper les défis potentiels, à prévenir les incidents et à assurer une exploitation efficace et sécurisée de ses processus métier.

Enfin au quatrième point, la gestion des risques opérationnels chez la Capital One garantit la production de rapports détaillés sur les résultats des risques opérationnels destinés aux hauts dirigeants de l'entreprise, au comité exécutif et au conseil d'administration. Cette pratique assure une transparence totale ainsi qu'une surveillance régulière des risques opérationnels à tous les niveaux de gouvernance de l'entreprise. En fournissant des rapports complets et précis sur les tendances, les incidents et les mesures d'atténuation, la Capital One permet à ses dirigeants de prendre des décisions éclairées et stratégiques pour gérer efficacement les risques opérationnels. Cette approche proactive contribue à renforcer la culture de gestion des risques au sein de

l'organisation et à assurer une prise de décisions pour préserver la stabilité et la durabilité des activités de l'entreprise.

4.3.31 Canada-Société Générale

Cette banque a établi surtout trois actions. En premier position, la Canada-Société Générale accorde une importance capitale à la sécurité de son système d'information, consciente de la menace de plus en plus prégnante que représente la cybercriminalité et des risques associés aux technologies de l'information. Dans cet esprit, l'entreprise s'engage à protéger de manière proactive non seulement ses propres données internes, mais aussi les informations sensibles de ses clients. Cette approche renforce la résilience du système d'information de Canada-Société Générale et contribue à maintenir la confidentialité, l'intégrité et la disponibilité des données essentielles.

Au second plan, protection des clients via *OPPENS*. Dans un effort continu pour renforcer la protection de ses clients, la Canada-Société Générale collabore avec la *start-up OPPENS* pour offrir des services de conseil et d'accompagnement en cybersécurité aux petites et moyennes entreprises (PME). Cette collaboration stratégique vise à aider les entreprises à améliorer leur posture de sécurité en ligne grâce à une plateforme numérique spécialisée dans la cybersécurité. En guidant les PME dans la mise en œuvre de mesures de sécurité efficaces et en les sensibilisant aux risques cybernétiques actuels, Canada-Société Générale témoigne de son engagement à protéger activement ses clients contre les menaces en ligne. Cette initiative démontre la volonté de la banque de jouer un rôle proactif dans la protection des entreprises clientes, en les aidant à se prémunir contre les cyber-risques et à maintenir un environnement numérique sécurisé pour leurs activités.

Au troisième plan, sensibilisation et Formation en cybersécurité. Au sein de son espace dédié à la « Sensibilisation et Formation », la Canada-Société Générale s'engage à fournir des conseils et une expertise de pointe en matière de cybersécurité. En mettant à disposition des ressources informatives et des programmes de formation spécialisés, l'entreprise vise à renforcer la sensibilisation et les compétences en matière de sécurité numérique, aussi bien en interne que pour ses clients. Cette démarche proactive démontre l'engagement de Canada-Société Générale à prévenir les cyber-risques, à promouvoir une culture de sécurité robuste et à équiper ses

collaborateurs et ses clients des outils nécessaires pour se prémunir contre les menaces en ligne. En offrant des conseils pertinents et des formations adaptées, la banque s'efforce de créer un environnement numérique sécurisé et de favoriser une utilisation responsable des technologies de l'information, aussi bien au sein de l'organisation que chez ses clients.

4.3.32 Caisses Populaires Acadiennes

Cette banque a mis en œuvre cinq mesures clés. Premièrement, au sein des Caisses Populaires Acadiennes, des politiques internes, des directives et des procédures spécifiques ont été soigneusement élaborées pour encadrer de manière rigoureuse la sécurité informatique et la gestion des risques associés aux cyberincidents. Ces documents servent de cadre de référence essentiel pour garantir la protection des données sensibles, la prévention des cyberattaques et la gestion efficace des incidents de sécurité. En établissant des normes claires et des protocoles détaillés, les Caisses Populaires Acadiennes démontrent leur engagement envers la sécurité de l'information et leur volonté de maintenir un environnement numérique sécurisé pour leurs membres et leur personnel. À travers ces politiques, directives et procédures, l'organisation renforce sa capacité à anticiper, identifier et répondre aux menaces cybernétiques, assurant ainsi la confidentialité, l'intégrité et la disponibilité des données critiques.

Au second rang, les Caisses Populaires Acadiennes ont déployé un système informatique sécurisé afin de protéger de manière proactive les données sensibles et de prévenir les cyberattaques. Ce système comprend diverses mesures de sécurité telles que des pares-feux, des systèmes de détection d'intrusion, des outils de surveillance continue, des protocoles de chiffrement et d'autres mécanismes de protection avancés. En intégrant ces technologies de pointe, les Caisses Populaires Acadiennes renforcent la sécurité de leur infrastructure informatique, garantissant ainsi la confidentialité et l'intégrité des informations critiques. En adoptant une approche multicouche de sécurité, l'organisation se positionne de manière proactive pour faire face aux menaces émergentes et pour assurer la protection des données de ses membres et de son personnel contre les cybermenaces.

En troisième rang, les Caisses Populaires Acadiennes accordent une importance primordiale au respect des règles et normes en matière de sécurité informatique pour assurer une protection

adéquate de leurs opérations contre les cybermenaces. En se conformant aux réglementations en vigueur, aux meilleures pratiques de l'industrie et aux normes de sécurité reconnues, l'organisation démontre son engagement à maintenir des environnements numériques sécurisés et conformes. En suivant ces directives établies, les Caisses Populaires Acadiennes renforcent leur posture de sécurité, réduisent les risques de non-conformité et préservent la confiance de leurs membres et partenaires en assurant la protection de leurs données sensibles.

Au quatrième rang, les Caisses Populaires Acadiennes ont mis en place un plan de continuité des affaires afin de garantir la résilience de leurs opérations en cas de cyberincident majeur. Ce plan complet comprend des mesures d'urgence et de rétablissement prévues pour limiter les pertes potentielles et assurer la reprise rapide des activités essentielles. En prévoyant des procédures détaillées, des stratégies de communication d'urgence, des sauvegardes régulières des données critiques et des tests de simulation périodiques, l'organisation se prépare de manière proactive à faire face à toute interruption majeure due à un incident de cybersécurité.

Enfin au cinquième rang, les Caisses Populaires Acadiennes ont établi des mécanismes de contrôle interne pour surveiller et évaluer de manière régulière l'efficacité de leurs mesures de sécurité et de prévention des cyberincidents. Ces mécanismes de contrôle comprennent la mise en place de processus d'évaluation continue, de revues de conformité périodiques, de tests de pénétration et d'audits de sécurité pour garantir que les politiques et les procédures en place sont efficaces et respectées. En renforçant ainsi leur capacité à détecter les vulnérabilités potentielles, à réagir rapidement aux menaces émergentes et à maintenir un environnement sécurisé, les Caisses Populaires Acadiennes démontrent leur engagement envers la protection des données sensibles et la prévention des cyberincidents. Ces contrôles internes jouent un rôle crucial dans la gestion proactive des risques et dans la garantie de la sécurité globale des opérations de l'organisation.

4.3.33 Alberta Treasury Branches (ATB)

Cette banque a élaboré quatre mesures essentielles. Tout d'abord, l'ATB reconnaît que le risque de cybersécurité peut découler de divers facteurs tels que le manque de formation, les vulnérabilités des fournisseurs, la non-conformité des contrôles de cybersécurité, la concentration des données, le manque de ressources, et d'autres encore. Cette identification proactive des sources potentielles

de risques de cybersécurité permet à ATB de cibler les domaines critiques nécessitant une attention particulière pour renforcer la sécurité de ses systèmes et données. En comprenant les diverses menaces possibles et en évaluant continuellement les facteurs de risque, ATB met en œuvre des stratégies de prévention et de mitigation efficaces pour réduire l'exposition aux cybermenaces et protéger ses activités et ses clients contre les attaques potentielles.

En deuxième lieu, l'ATB adopte une perspective interdisciplinaire en considérant le risque de cybersécurité comme une préoccupation transversale. Cela implique l'alignement de tous les aspects de l'entreprise afin de soutenir des pratiques de cybersécurité efficaces. En intégrant les perspectives et les expertises de différentes disciplines au sein de l'organisation, ATB peut garantir une approche holistique de la cybersécurité, couvrant non seulement les aspects techniques, mais aussi les éléments humains, organisationnels et de gouvernance. En favorisant la collaboration entre les équipes et en encourageant une culture de sécurité partagée, ATB renforce sa capacité à anticiper, prévenir et répondre aux menaces cybernétiques de manière coordonnée et intégrée.

Pour le troisième point, l'ATB met l'accent sur le développement d'une approche durable et résiliente pour la gestion des risques de cybersécurité concernant ses employés, ses clients, son infrastructure et ses actifs. Cela implique la conception de politiques robustes, la mise en œuvre de contrôles de sécurité efficaces, une gouvernance rigoureuse et une évaluation régulière de l'efficacité des mesures de protection mises en place. En adoptant cette approche globale et proactive, ATB vise à garantir la continuité des activités, à réduire les impacts potentiels des cyberincidents et à assurer une protection optimale des données et des systèmes contre les menaces en constante évolution.

Pour le quatrième plan, l'ATB accorde une priorité significative aux investissements et aux ressources dédiés à la réduction des expositions aux risques de cybersécurité à des niveaux acceptables, conformément à son appétit pour le risque. L'organisation a mis en place un programme de gestion des risques de cybersécurité visant à identifier et à remédier aux vulnérabilités, tout en protégeant efficacement les actifs de l'entreprise. En allouant des ressources adéquates pour renforcer la sécurité des systèmes, pour former le personnel et pour mettre en œuvre des contrôles de sécurité robustes, ATB démontre son engagement envers la protection proactive contre les cybermenaces. En investissant de manière stratégique dans la cybersécurité, ATB

renforce sa résilience organisationnelle et sa capacité à faire face aux menaces émergentes, garantissant ainsi la sécurité des données et la confiance de ses parties prenantes.

Enfin au cinquième point, l'ATB renforce sa résilience face aux cyberattaques en étendant ses capacités de défense grâce à des partenariats stratégiques avec des fournisseurs de cybersécurité renommés. De plus, l'organisation propose une formation obligatoire de sensibilisation à la cybersécurité à l'ensemble de son équipe pour renforcer la culture de la sécurité. En s'associant avec des experts du domaine et en fournissant une formation continue à son personnel, ATB démontre son engagement à rester à la pointe des meilleures pratiques en matière de cybersécurité. Cette approche proactive vise à renforcer la posture de sécurité de l'entreprise, à sensibiliser efficacement les collaborateurs aux menaces numériques et à promouvoir une culture d'engagement envers la protection des données et des systèmes.

4.3.34 Citi Canada

Cette banque a fixé essentiellement quatre orientations. Premièrement, la Citi Canada a mis en place une stratégie axée sur les menaces pour se protéger contre les cyberattaques, détecter et répondre aux incidents, ainsi que pour se remettre rapidement en cas d'incident. L'organisation reconnaît la sophistication croissante des tactiques utilisées par les acteurs malveillants, ainsi que l'évolution des technologies employées pour mener des transactions financières, les exposant ainsi à des risques accrus de cyberattaques et d'incidents de sécurité. En adoptant une approche proactive et axée sur les menaces, Citi Canada cherche à identifier et à atténuer les risques, à renforcer sa posture de sécurité et à garantir la protection de ses données sensibles. Cette orientation stratégique lui permet de rester agile face aux menaces en constante évolution et de réagir de manière efficace pour maintenir la confiance de ses clients et assurer la sécurité de ses opérations financières.

Deuxièmement, gestion du risque en trois lignes de défense. La Citi Canada a mis en place un programme de gestion des risques liés aux technologies et à la cybersécurité qui repose sur trois niveaux de protection. Le premier niveau, placé sous l'autorité de l'office du responsable de la sécurité des informations, propose des mesures de contrôle et des capacités techniques et opérationnelles pour se prémunir contre les risques cybernétiques, répondre aux incidents et gérer les violations de données. Le deuxième niveau de défense, composé d'unités de gestion des risques

indépendantes, fonctionne de manière autonome par rapport au premier niveau. Sa mission principale est de surveiller les activités à risque du premier niveau et de les remettre en question, tandis que la gestion des risques indépendante s'occupe d'identifier, de mesurer, de surveiller, de contrôler et de rapporter de manière autonome les risques globaux. Ces unités établissent également des normes pour la gestion des risques et la surveillance, comprenant la gestion indépendante des risques et la gestion indépendante des risques de conformité, supervisées respectivement par le *Chief Risk Officer* (CRO) et le *Chief Compliance Officer* (CCO). Ces responsables ont un accès direct au Conseil et à sa gestion des risques pour s'acquitter efficacement de leurs responsabilités, notamment en remontant les problèmes critiques au conseil si nécessaire. La troisième ligne de défense est l'audit interne, qui est indépendant des premier et deuxième niveau de protection ainsi que des fonctions de soutien de l'entreprise. Son objectif est de fournir de manière rapide et objective au conseil d'administration, au comité d'audit, à la direction de Citi et aux régulateurs une assurance indépendante concernant l'efficacité de la gouvernance, de la gestion des risques et des contrôles atténuant les risques actuels et émergents, tout en améliorant la culture de contrôle au sein de Citi. L'auditeur en chef gère les activités d'audit interne et rend compte fonctionnellement au président du comité d'audit de Citi, ainsi qu'administrativement au PDG de Citi. L'auditeur en chef bénéficie d'un accès direct au conseil d'administration et au comité d'audit pour aborder les risques et problèmes découverts au cours des audits internes (P.61).

Troisièmement, chez la Citi Canada, les équipes dédiées au risque opérationnel technologique, au risque cybernétique et à la conformité indépendante en matière de technologie et de sécurité de l'information jouent un rôle essentiel en évaluant, anticipant et mettant en question les pratiques et capacités d'atténuation des risques. Elles réalisent des évaluations des risques technologiques et de cybersécurité, surveillent en permanence les exigences légales et réglementaires, identifient les risques émergents, et mènent des évaluations de l'assurance des risques liés à la cybernétique. En assurant une surveillance et une évaluation continues, ces équipes contribuent à renforcer la posture de sécurité de Citi, à anticiper les menaces potentielles, à identifier les domaines à risque et à garantir la conformité aux normes réglementaires en vigueur. Leur rôle est crucial pour assurer la protection des données et des activités de l'entreprise contre les cybermenaces et pour maintenir un haut niveau de sécurité en matière de technologie et d'information.

Quatrièmement, contrôle interne et assurance indépendante. L'audit interne agit comme la troisième ligne de défense en fournissant une assurance indépendante sur la gestion du risque de cybersécurité par l'organisation dans son ensemble. En collaboration avec d'autres fonctions de contrôle interne, l'audit interne joue un rôle crucial dans l'évaluation des pratiques de gestion des risques de cybersécurité et dans la garantie de la conformité aux politiques et aux normes établies. De plus, Citi a mis en place des comités de haut niveau. Comme exemple le Comité des risques liés à la sécurité de l'information qui supervise la tolérance au risque de l'entreprise en matière de cybersécurité. Ces comités assurent une surveillance continue de la gestion des risques de cybersécurité, évaluent les politiques et les stratégies de sécurité de l'information, et veillent à ce que l'entreprise maintienne une position robuste face aux menaces cybernétiques. En renforçant le contrôle interne et en assurant une assurance indépendante, Citi s'efforce de garantir efficacement la protection de ses données, de ses actifs et de ses opérations contre les risques de cybersécurité.

Enfin cinquièmement, le conseil d'administration de Citi, ainsi que ses comités spécialisés, exercent une gouvernance active en supervisant les efforts de la direction pour atténuer les risques de cybersécurité et gérer les incidents cybernétiques. Le conseil d'administration reçoit régulièrement des rapports détaillés sur la cybersécurité, participant ainsi à des discussions approfondies tout au long de l'année pour évaluer l'efficacité du programme de cybersécurité de Citi. En maintenant une surveillance continue et en s'engageant de manière proactive dans la gouvernance de la cybersécurité, le conseil d'administration assure une direction stratégique et décisionnelle pertinente pour garantir la résilience de l'organisation face aux menaces numériques.

.

CONCLUSION

Ce dernier chapitre présente une vue d'ensemble des résultats. Cette étude s'est concentrée sur les risques associés à la cybersécurité et à la protection des renseignements personnels rencontrés par les banques canadiennes. L'analyse a démontré que toutes les institutions bancaires examinées avaient divulgué des informations concernant ces risques dans leurs rapports annuels. En outre, notre recherche a mis en lumière plusieurs risques significatifs et des mesures spécifiques mises en place par les banques pour atténuer ces menaces. Nous avons examiné les rapports annuels de 2020, 2021 et 2022 de trente-quatre des plus de soixante banques opérant au Canada, afin d'identifier les différents risques ainsi que les mesures d'atténuation mises en œuvre pour les gérer.

La revue de littérature présentée dans le premier chapitre a fourni un cadre essentiel en proposant un aperçu des différentes formes de cybercriminalité, des technologies adoptées pour assurer la cybersécurité, ainsi que des lois et réglementations s'appliquant à la protection des renseignements personnels. Cette première analyse a également mis en évidence le rôle crucial de la gestion des risques pour atténuer les cybermenaces et protéger les informations sensibles.

Dans le second chapitre, nous avons établi le cadre théorique de notre recherche, en nous appuyant sur la théorie de la signalisation et le cadre conceptuel des risques. La théorie de la signalisation a permis d'explorer comment les entreprises peuvent utiliser la divulgation d'informations pertinentes pour susciter la confiance des investisseurs et améliorer leur image institutionnelle. En parallèle, le cadre conceptuel des risques a fourni un cadre méthodologique pour identifier, évaluer et gérer les risques auxquels se confrontent les banques.

La méthodologie, décrite dans le troisième chapitre, a mis en œuvre une approche qualitative pour analyser les rapports annuels des banques sélectionnées, prenant en compte divers facteurs tels que la taille de l'institution, son expérience en matière de cybercriminalité et sa présence sur le territoire canadien, y compris au Québec. Cette sélection a permis d'obtenir une vision représentative de la gestion des risques au sein du secteur bancaire.

Dans notre quatrième chapitre, nous avons présenté les résultats de notre analyse visant à comprendre la manière dont les banques canadiennes divulguent les risques liés à la protection des

renseignements personnels et les stratégies défensives qu'elles mettent en place pour gérer ces risques. Cela inclut l'inventaire, la divulgation des risques, et les mesures de sécurité mises en œuvre pour la protection des données personnelles. Nos résultats ont révélé que toutes les banques canadiennes avaient abordé effectivement les risques liés à la protection des renseignements personnels dans leurs rapports. Cela répond à notre première question de recherche sur l'utilisation de la divulgation proactive des risques pour renforcer la confiance des clients et des investisseurs. En identifiant et en divulguant ces risques, les banques démontrent une transparence qui pourrait renforcer cette confiance.

Les principaux risques identifiés incluent : Le manque de connaissances concernant les mises à jour et les meilleures pratiques en matière de protection des renseignements personnels, la modification des lois et règlements ainsi que la complexité de leur interprétation, des questions de sécurité de l'information, de cybersécurité et des technologies de l'information, le perfectionnement des technologies et des stratégies d'attaque, la complexité des systèmes et des processus de collecte et de stockage des données, la sécurité infonuagique, la non-conformité aux lois et réglementations ainsi que la dépendance à la technologie et aux tiers.

Les banques ont indiqué la nécessité d'améliorer la sensibilisation de leurs employés et les maintenir informés des dernières pratiques et des meilleures pratiques en matière de cybersécurité et de protection des données. Elles ont signalé des difficultés à se tenir au courant des changements réglementaires et à interpréter les lois et les règlements complexes liés à la protection des renseignements personnels. Les banques ont identifié le risque de compromission des données sensibles de leurs clients et ont souligné l'importance de renforcer leurs systèmes de sécurité de l'information et de mettre en place des processus de gouvernance et de contrôle des risques robustes. Elles ont également fait état du risque lié à l'évolution constante des technologies et des stratégies d'attaque, ce qui nécessite des investissements continus dans la cybersécurité et la mise en place de mesures proactives pour atténuer les menaces émergentes. Les banques ont souligné l'importance de se tenir au courant des nouvelles technologies et des stratégies d'attaque et d'investir dans des solutions de cybersécurité avancées pour rester à l'avant-garde des menaces émergentes. Elles ont fait état du risque que les systèmes complexes et les processus de collecte et de stockage de données puissent entraîner des vulnérabilités et des erreurs ainsi ont mis en évidence le risque lié à la sécurité infonuagique et souligné l'importance de mettre en place des politiques et

des pratiques de sécurité robustes pour protéger les données stockées dans le cloud. Les banques ont également fait état du risque de ne pas respecter les lois et les réglementations en matière de protection des renseignements personnels. Les banques ont signalé le risque lié à la dépendance envers des tiers pour les technologies et les services critiques, et ont souligné la mise en œuvre des évaluations rigoureuses des fournisseurs et partenaires pour garantir que ces entités adhèrent aux normes de sécurité et de confidentialité requises.

Cela démontre que les banques canadiennes disposent de stratégies claires qui renforcent leur capacité à gérer les risques liés à la protection des renseignements personnels et à faire face aux cybermenaces, ce qui répond à notre question de recherche sur les stratégies défensives mise en place.

Nos contributions à la recherche incluent une meilleure compréhension des pratiques de divulgation des risques liés à la protection des renseignements personnels dans le secteur bancaire canadien. Cela devrait améliorer les politiques et pratiques de gestion des risques tout en renforçant la confidentialité, l'intégrité des données des clients, et la confiance du public dans le système financier du pays.

Cependant, notre étude est limitée par sa dépendance aux informations des rapports annuels des banques, ce qui signifie que certaines données internes et spécifiques pourraient ne pas être incluses. Cela pourrait limiter la portée de notre analyse. Pour les recherches futures, il serait intéressant d'explorer des données internes plus approfondies des banques, mener des études de cas sur des incidents spécifiques, ou encore comparer les pratiques canadiennes avec celles d'autres pays pour évaluer les différences et les similitudes dans la gestion des risques liés à la protection des renseignements personnels.

En récapitulant ces éléments, notre recherche a non seulement mis en exergue les risques auxquels sont confrontées les banques canadiennes en matière de cybersécurité, mais a aussi fourni des mesures pratiques pour leur gestion des risques. Il est essentiel que les banques prennent des mesures proactives pour renforcer leurs systèmes de sécurité et leur capacité d'adaptation aux évolutions technologiques et réglementaires. Ce mémoire contribue ainsi à une meilleure compréhension des défis et des opportunités en matière de cybersécurité dans le secteur bancaire

canadien, tout en soulignant l’importance d’une approche intégrée et dynamique pour garantir la sécurité des renseignements personnels de leurs clients

Figure 1: Nombre total d'utilisateurs des réseaux sociaux (Rapleaf's data)

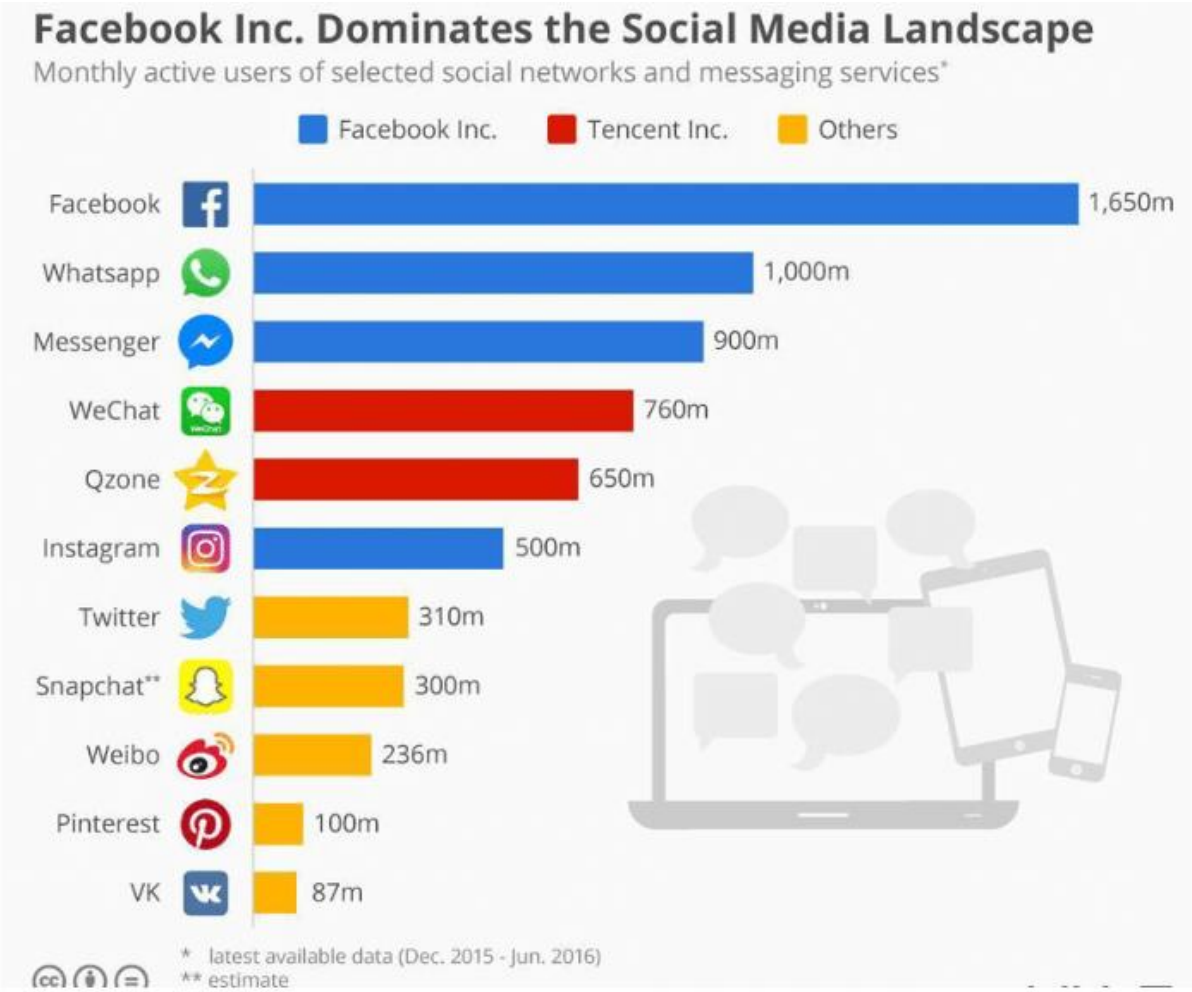
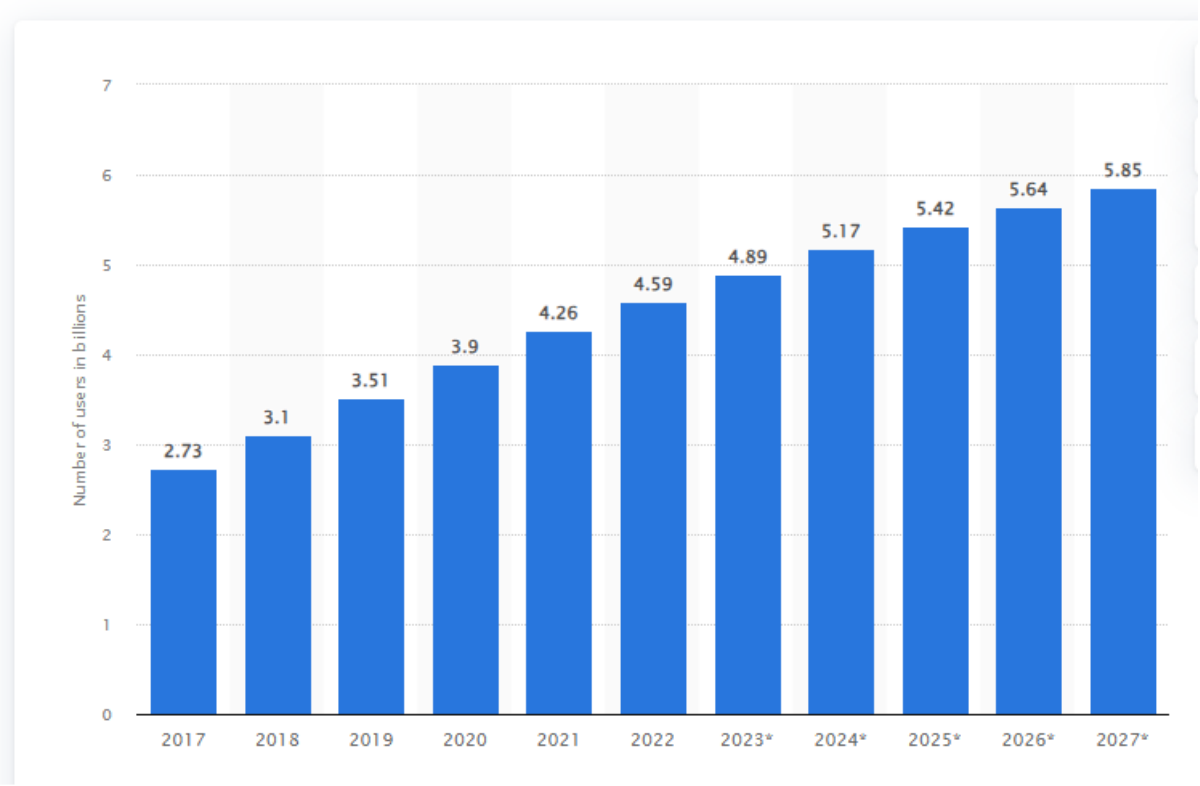


Figure 2 : Nombre d'utilisateurs de réseaux sociaux dans le monde de 2017 à 2027 en milliards (Published by Stacy Jo Dixon, Aug 29, 2023)



BIBLIOGRAPHIE

Akkour, S., Assadi, F., & Haounani, A. (2023). Protection des données personnelles et cybersécurité. Revue Internationale du Chercheur, 4(3). https://revuechercheur.com/index.php/home/article/view/664

Akkour, S., Haounani, A., & Assadi, F. (2023). La protection des données personnelles face à l'intelligence artificielle. Revue Internationale du Chercheur, 4(3), Article 3.

Allen, S. (2003). Financial risk management: a practitioner's guide to managing market and credit risk (with CD-ROM) (vol. 119). John Wiley & Sons. https://books.google.com/books?hl=fr&lr=&id=V_MAG8VAi-YC&oi=fnd&pg=PR15&dq=financial+risk+management+practitioner%27s+guide&ots=6AYq_qJEKh&sig=gex_kVS2dnwx07tfhZevXqQ8yMA

Alford, C. F. (2002). Whistleblowers: Broken lives and organizational power. Cornell University Press. https://books.google.com/books?hl=fr&lr=&id=H8Z1AIRxdE0C&oi=fnd&pg=PR5&dq=C.+Fred+Alford+-+L%27auteur+de+%22Whistle-Blowers:+Broken+Lives+and+Organizational+Power%22+offre+une+analyse+approfondie+des+enjeux+psychologiques,+%C3%A9thiques+et+organisationnels+li%C3%A9s+%C3%A0+la+divulgation+d%27informations+sensibles.&ots=bsjC6Fubjw&sig=3_C00PWgFpy08vRIZqW2z7FtqgY

Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., & Janicke, H. (2020). A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom. Applied Sciences, 10(10), 3660.

André-Laurendeau, C. (2023). Politique sur la protection des renseignements personnels. https://eduq.info/xmlui/bitstream/handle/11515/38999/politique-protection-renseignements-personnels-andre-laurendeau.pdf

Ann Cavoukian. (2023). Protection de la vie privée dès la conception. In Wikipédia. https://fr.wikipedia.org/w/index.php?title=Protection_de_la_vie_priv%C3%A9e_d%C3%A8s_la_conception&oldid=203734003

Armstrong, C. S., Guay, W. R., & Weber, J. P. (2010). The role of information and financial reporting in corporate governance and debt contracting. Journal of accounting and economics, 50(2-3), 179-234.

Aubin, N. (2023). Les tensions entre les principes juridiques applicables aux systèmes d'intelligence artificielle en droit québécois (explicabilité, exactitude, sécurité et équité). https://papyrus.bib.umontreal.ca/xmlui/handle/1866/28164

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation

Bahl, L., Gagné, V., & Corriveau, A. (2021). Cybersécurité, légitimité et étendue de la divulgation aux rapport annuels d'entreprises canadiennes. https://qc.search.yahoo.com/yhs/search?p=Bahl%2C%20L.%2C%20Gagn%C3%A9%2C%20V.%20et%20Corriveau%2C%20A.%20(2021).%20Cybers%C3%A9curit%C3%A9%2C%20l%C3%A9gitimit%C3%A9%20et%20%C3%A9tendue%20de%20la%20divulgation%20aux%20rapport%20annuels%20d%E2%80%99entreprises%20canadiennes.%20La%20fuite%20de%20donn%C3%A9es%20personnelles%20chez%20Desjardins.%2041%C3%A8me%20congr%C3%A8s%20de%20l%E2%80%99AFC%2C%20mai.&hspart=fc&hsimp=yhs-90&type=fc_AA30D90E577_s69_g_e_d_n1_c999&param1=7&param2=eJwtjs1uwjAQhF9ljyBhs%2BvYjk1OKZQHqHoq4mCCG6z8KglK1aevXaE9zOy3s9LU4X4prh8nQpSW7GV37eNOUROPUkWxNh3CGK3WnDLkZA0npSOt%2FRBx5aJ9uui64Te0rdsrjrBZQ38f1hn6BQg5FhCBlgX8aLkFN46tX%2F2tCcteZTnPNGyax9K1O2hD46H2VTNsoXpMQ%2Bf3JHKOaWB2324Kr5fUaw6vrs%2FZT%2F%2B%2BVEeD1iKTZCwjej8zk78hO55Ii7MRpTZlylcpLFBIhjkj%2BYnikMmDIm6l%2BvoDsDdRQg%3D%3D

Barkat, S. (2017). La relation de la gestion des risques financiers et la gouvernance des banques: Roa Iktissadia Review, 7(1), Article 1.

Belkacemie, F. (2017). Apport de l'audit interne a la performance des entreprises industrielles algeriennes. https://dspace.univ-alger3.dz/jspui/handle/123456789/6933

Benaroch, M. (2021).Third-party induced cyber incidents - much ado about nothing?

Bendjeddou, C., Lekikot, A., & Benziadi, D. (encadreur). (2014). L'évaluation de la pratique de l'audit interne dans les banques publiques [Thesis]. http://dspace.esc-alger.dz:8080/xmlui/handle/123456789/1391

Bendovschi, A. (2015). Cyber-attacks–trends, patterns and security countermeasures. Procedia Economics and Finance, 28, 24-31.

Bensoussan, A. (2018). Règlement européen sur la protection des données : Textes, commentaires et orientations pratiques. Bruylant.

Botosan, C. A., & Plumlee, M. A. (2002). A Re‐examination of Disclosure Level and the Expected Cost of Equity Capital. Journal of Accounting Research, 40(1), 21-40. https://doi.org/10.1111/1475-679X.00037

Boutemadja, B. (2013). L'audit interne. Lulu.com.

Branco, M. C., & Rodrigues, L. L. (2006). Communication of corporate social responsibility by Portuguese banks: A legitimacy theory perspective. Corporate communications: An international journal, 11(3), 232-248.

Bromiley, P., Rau, D. et McShane, M. K. (2016). Can strategic risk management contribute to enterprise risk management. A strategic management perspective. A Strategic

Management Perspective (October 20, 2014). Forthcoming: Bromiley, P., Rau, D., and Mcshane, M, 140-156.

Cacciapaglia, K. (2018). Analyse sur les différentes cyberattaques informatiques [PhD Thesis, Haute école de gestion de Genève]. https://doc.rero.ch/record/323723/files/Cacciapaglia_tdb_heg_2018.pdf

Calderon, T. G., & Gao, L. (2021). Cybersecurity risks disclosure and implied audit risks : Evidence from audit fees. International Journal of Auditing, 25(1), 24-39. https://doi.org/10.1111/ijau.12209

Canada, C. à la protection de la vie privée du. (2021, février 11). La Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE). https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/

Carbonneau, M. (2022). L'évaluation des risques et des préjudices portés à la vie privée en contexte de transformation numérique : Considérations éthiques autour de la Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (Loi 25) [PhD Thesis, Université du Québec à Rimouski]. https://semaphore.uqar.ca/id/eprint/2129/

Cavoukian, A. (2009). Privacy by design: The 7 foundational principles. Information and privacy commissioner of Ontario, Canada, 5, 12.

Chen, J., Henry, E., & Jiang, X. (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

Cirano, & Bernard, J.-G. (2002). Le risque : Un modèle conceptuel d'intégration. CIRANO. https://www.cirano.qc.ca/files/publications/2002RP-16.pdf

Cisco, C. (2018). Annual cybersecurity report. Pg, 8, 19.

Colasse, B. (2004). Harmonisation comptable internationale : De la résistible ascension de l'IASC/IASB. Gérer et comprendre, 75, 30-40.

Collins, L., & Valin, G. (1992). Audit et contrôle interne : Aspects financiers, opérationnels et stratégiques. Dalloz.

Comeau, P. A. (2009). Protection des renseignements personnels : Privacy protection : beyond the blueprint. https://policycommons.net/artifacts/1234852/protection-des-renseignements-personnels/1787923/

COSO. (2023). In Wikipédia. https://fr.wikipedia.org/w/index.php?title=COSO&oldid=204303920#Le_r%C3%A9f%C3%A9rentiel_COSO_(Internal_Control_%E2%80%93_Integrated_Framework)

Côté-Freeman, S. (2019). L'état de la GRE au Canada : Enquête d'étalonnage.

Couldry, N., & Mejias, U. A. (2020). The costs of connection: How data are colonizing human life and appropriating it for capitalism. Oxford University Press. https://academic.oup.com/sf/article-abstract/99/1/e6/5781190

Creswell, J. W., & Creswell, J. D. (2017). Research design: Qualitative, quantitative, and mixed methods approaches. Sage publications.

Culioli, M., Libes, M., Mouthuy, T., & Kourilsky, M. (2009). Elaboration d'une PSSI au sein d'une unité propre du CNRS : Utilisation de la méthode EBIOS.

Cybersécurité - 5e éd. : Sécurité informatique et réseaux. (2016). Dunod.

Dainelli, F., Bini, L., & Giunta, F. (2013). Signaling strategies in annual reports : Evidence from the disclosure of performance indicators. Advances in Accounting, 29(2), 267-277. https://doi.org/10.1016/j.adiac.2013.09.003

De Coussergues, S., Bourdeaux, G., & Gabteni, H. (2020). Gestion de la banque-9e éd. : Tous les principes et outils à connaître. Dunod. https://books.google.com/books?hl=fr&lr=&id=P2z2DwAAQBAJ&oi=fnd&pg=PT387&dq=De+Coussergues+S.,+Bourdeaux+G.+et+Gabten+H.+(2020).+Tous+les+principes+et+outils+%C3%A0+conna%C3%AEtre.+Gestion+de+la+banque+-+9e+%C3%A9d&ots=kq_VEe1-ER&sig=4YMiTgMDe-YlHoKEO3nRZhm-QwA

Dionne, G. (2015). La gouvernance de la gestion des risques : Quoi de neuf ? Gestion, 40(1), 40-45. https://doi.org/10.3917/riges.401.0040

Dupont, B., & Gagnon, B. (2008). La sécurité précaire des données personnelles en Amérique du Nord. http://benoitdupont.openum.ca/files/sites/31/2015/07/securiteprecaire.pdf

Echoso, J. (2024). Cybersécurité en 2024 : Les meilleurs outils et stratégies pour protéger vos données dans le paysage actuel des menaces. Joël Echoso.

ECIIA, A. İ. D. E. K. (2005). European Confederation of Institutes of Internal Auditing. Konum Raporu, Avrupa'da İç Denetim.

Eddine, T. D., & Ouassim, L. (s. d.).(2023) Les principaux facteurs du risque technologique et leurs impacts sur la finance moderne. Consulté 12 avril 2024, à l'adresse https://www.researchgate.net/profile/Djamel-Eddine-Terfas/publication/369374774_Les_principaux_facteurs_du_risque_technologique_et_leu

rs_impacts_sur_la_finance_moderne/links/641867cf66f8522c38bd78b7/Les-principaux-facteurs-du-risque-technologique-et-leurs-impacts-sur-la-finance-moderne.pdf

Eijkelenboom, E. V. A., & Nieuwesteeg, B. F. H. (2021). An analysis of cybersecurity in Dutch annual reports of listed companies. Computer Law & Security Review, 40, 105513.

Fombrun, C. J. et Van Riel, C. B. (2004). Fame & fortune: How successful companies build winning reputations. FT press. https://books.google.com/books?hl=fr&lr=&id=7iZcLsu5HxgC&oi=fnd&pg=PR17&dq=Fombrun,+et+Van+Riel,+2004&ots=HXrPn9cKfR&sig=PLvaLHumotH0FbdQmSiZZRqhmKc

Familoni, B. T., & Shoetan, P. O. (2024). Cybersecurity in the financial sector : A comparative analysis of the USA and Nigeria. Computer Science & IT Research Journal, 5(4), 850-877.

Fernandez-Bollo, É. (2015). Institutions financières et cybercriminalité. Revue d'économie financière, 120(4), 181-198. https://doi.org/10.3917/ecofi.120.0181

Fisher, R., Wood, J., Porod, C., & Greco, L. (2019). Evaluating cyber risk reporting in US financial reports. Cyber Security: A Peer-Reviewed Journal, 3(3), 275-286.

Flaherty, D. H. (2001). La Loi sur la protection des renseignements personnels et les documents électroniques (la Loi) et la communauté archivistique canadienne : Guide et commentaire. Victoria (C.-B.), 8, 1R1.

Fréminville, M. de. (2019). La cybersécurité et les décideurs : Sécurité des données et confiance numérique. ISTE Group.

Freyssinet*, É. (2013). L'Internet des objets : Un nouveau champ d'action pour la cybercriminalité. Réalités industrielles, 2, 66-69.

Frigo, M. L., & Anderson, R. J. (2011). Strategic risk management: A foundation for improving enterprise risk management and governance. Journal of Corporate Accounting & Finance, 22(3), 81-88. https://doi.org/10.1002/jcaf.20677

Gera, J., & Battula, B. P. (2018). Detection of spoofed and non-spoofed DDoS attacks and discriminating them from flash crowds. EURASIP Journal on Information Security, 2018(1), 9. https://doi.org/10.1186/s13635-018-0079-6

Germond, B. P., & Bonnault, R. (1987). Révision et certification des comptes. Masson.

Ghernaouti, S. (2016). Cybersécurité - 5e éd. : Sécurité informatique et réseaux. Dunod.

Gola, R. (2017). Le règlement européen sur les données personnelles, une opportunité pour les entreprises au-delà de la contrainte de conformité. LEGICOM, 59(2), 29-38. https://doi.org/10.3917/legi.059.0029

Gouvernement du Canada, B. du vérificateur général du C. (2017, mai 16). Rapport 1—Gérer le risque de fraude. https://www.oag-bvg.gc.ca/internet/Francais/parl_oag_201705_01_f_42223.html

Gouvernement du Québec. (2023, septembre). Définitions de mots en lien avec la protection des renseignements personnels. Gouvernement du Québec. https://www.quebec.ca/gouvernement/travailler-gouvernement/travailler-fonction-publique/services-employes-etat/conformite/protection-des-renseignements-personnels/definitions-concepts/lexique

Gril, E. (2021). Les leçons du vol de données chez Desjardins. Gestion, 45(4), 113-114.

Guedrib Ben Abderrahmen, M. (2013). Impact des mécanismes internes de gouvernance sur le risque fiscal : Une étude menée dans le contexte tunisien [PhD Thesis, Besançon]. https://www.theses.fr/2013BESA0002

Guinchard, A. (2015). Corporations confronted to cybercrime. Approaches of European and International Laws. (L'Entreprise Face À La Cybercriminalité. Approches De Droits International Et Européen). Approaches of European and International Laws.(L'Entreprise Face À La Cybercriminalité. Approches De Droits International Et Européen)(October 13, 2014). Droit pénal et nouvelles technologies, sous la direction de Jean-Paul Céré, Joan Miquel Rascagnères et Etienne Vergès (eds), L'Harmattan, 11, 11-34.

Gumb, B., & Noël-Lemaître, C. (2007). Le rapport des dirigeants sur le contrôle interne à l'épreuve de l'analyse de discours. Comptabilité Contrôle Audit, 13(2), 97-126. https://doi.org/10.3917/cca.132.0097

Hillson, D. (2017). Managing risk in projects. Routledge. https://www.taylorfrancis.com/books/mono/10.4324/9781315249865/managing-risk-projects-david-hillson

Hammarberg, K., Kirkman, M., & De Lacey, S. (2016). Qualitative research method: When to use them and how to judge them. Human reproduction, 31(3), 498-501.

Haouat Asli, M. (2011). Risque opérationnel bancaire : Le point sur la réglementation prudentielle. Management & Avenir, 48(8), 225-238. https://doi.org/10.3917/mav.048.0225

Hogg, P. W. (2007). Constitutional law of Canada. Thomson Carswell. https://digitalcommons.osgoode.yorku.ca/faculty_books/219/

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2022). Cybercrime and digital forensics: An introduction. Routledge. https://www.taylorfrancis.com/books/mono/10.4324/9780429343223/cybercrime-digital-forensics-thomas-holt-adam-bossler-kathryn-seigfried-spellar

https://www.assnat.qc.ca/fr/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html?appelant=MC consulté :2024-06-06 à 09:42:25. (s. d.). Projet de loi n° 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels—Assemblée nationale du Québec. Consulté 6 juin 2024, à l'adresse https://www.assnat.qc.ca/fr/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html?appelant=MC

https://www.quebec.ca/nouvelles/actualites/details/loi-25-sur-la-protection-des-renseignements-personnels-des-citoyens-du-quebec-entree-en-vigueur-de-nouvelles-dispositions-qui-font-du-quebec-un-chef-de-file-mondial-50726. (s. d.). Loi 25 sur la protection des renseignements personnels des citoyens du Québec—Entrée en vigueur de nouvelles dispositions qui font du Québec un chef de file mondial. Gouvernement du Québec. Consulté 16 mai 2024, à l'adresse https://www.quebec.ca/nouvelles/actualites/details/loi-25-sur-la-protection-des-renseignements-personnels-des-citoyens-du-quebec-entree-en-vigueur-de-nouvelles-dispositions-qui-font-du-quebec-un-chef-de-file-mondial-50726

Hubbard, D. W., & Seiersen, R. (2023). How to measure anything in cybersecurity risk. John Wiley & Sons. https://books.google.com/books?hl=fr&lr=&id=7B-uEAAAQBAJ&oi=fnd&pg=PR1&dq=Douglas+Hubbard+&ots=BDpgOKalqt&sig=AOxCPpXBlgf3Ut652myEMoF7dog

Iat, A. (2020). Comment les marchés financiers réagissent aux cyberattaques impactant les sociétés financières? https://hal.science/hal-02881359/document

Jawadi, F. (2010). Financial crises, bank losses, risk management and audit : What happened? Applied Economics Letters, 17(10), 1019-1022. https://doi.org/10.1080/13504850802676215

Kablan, S., Oulaï, A., & Mignault, P. (2023). L'évaluation des facteurs relatifs à la vie privée : Pour un équilibre entre l'objectif de protection des renseignements personnels et la responsabilité des entreprises. Les Cahiers de droit, 64(2), 397-437. https://doi.org/10.7202/1101118ar

Kalakuntla, R., Vanamala, A. B., & Kolipyaka, R. R. (2019). Cyber Security. HOLISTICA – Journal of Business and Public Administration, 10(2), 115-128.

Karfoul, H., & Lamarque, É. (2011). Proposition d'une mesure de l'efficacité du système de contrôle interne d'un établissement bancaire. Management & Avenir, 48(8), 362-381. https://doi.org/10.3917/mav.048.0362

Khalil, A., Abdelli, M.-E.-A., Slimene, I. B., & Ajili, W. (2022). Comprendre et mettre en oeuvre le contrôle interne : Réglementation, concepts et applications. Dunod.

Khoury, S. (2023). Évaluation des cybermenaces nationales 2023–2024. 23.

Kumar, S., & Somani, V. (2018). Social media security risks, cyber threats and risks prevention and mitigation techniques. International Journal of Advance Research in Computer Science and Management, 4(4), 125-129.

Kurii, Y., & Opirskyy, I. (2022). Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001: 2013. NIST Spec. Publ, 800(53), 10.

Lagare, S. (2021). Études des cyberattaques de type ransomware et proposition de solutions adaptées aux particuliers et PME [PhD Thesis, Haute école de gestion de Genève]. https://doc.rero.ch/record/333433/files/Travail_de_bachelor_Sara_Lagare_modifi_.pdf

Lajili, K., & Zéghal, D. (2005a). A Content Analysis of Risk Management Disclosures in Canadian Annual Reports. Canadian Journal of Administrative Sciences / Revue Canadienne Des Sciences de l'Administration, 22(2), 125-142. https://doi.org/10.1111/j.1936-4490.2005.tb00714.x

Lajili, K., & Zéghal, D. (2005b). Gérer le risque à l'échelle de l'entreprise: L'autre facette de la gouvernance d'entreprise. Gestion, 30(3), 104-114. https://doi.org/10.3917/riges.303.0104

Lamkaraf, I., & Houria, Z. (2019). L'audit interne au service de la gouvernance d'entreprise. Revue du contrôle, de la comptabilité et de l'audit, 3(2). https://revuecca.com/index.php/home/article/view/369

Landreville, O. D. (2023). Développement d'un outil d'évaluation de la conformité des PME à la Loi 25 [PhD Thesis, Université de Sherbrooke]. https://savoirs.usherbrooke.ca/bitstream/handle/11143/20627/denault_landreville_olivier_MSc_2023.pdf?sequence=8

Le Maux, J. (2019). La fraude à l'ère numérique. Gestion, 44(3), 48-55.

Lemieux, M. (2015). Cyber crime, governance and liabilities in the banking and payment industries. Banking & Finance Law Review, 31(1), 113.

Leray, C. (2008). L'analyse de contenu : De la théorie à la pratique, la méthode Morin-Chartier. PUQ. https://books.google.com/books?hl=en&lr=&id=9heHNhO1fSEC&oi=fnd&pg=PR7&dq=),+l%E2%80%99analyse+de+contenu+est+particuli%C3%A8rement+efficace+pour+examiner+comment+les+organisations+communiquent+des+informations+sur+la+gestion+des+risques&ots=VszOiolskJ&sig=yBH3PduZE7PL6pJD8DADj_0efNE

Levac, S. E. (2023). Projet de loi C-27 – Loi de 2022 sur la mise en œuvre de la Charte du numérique C'O. https://policycommons.net/artifacts/8246597/projet-de-loi-c-27/9163536/

Luo, Xueming and Naveen Donthu (2006), "Marketing's Credibility: A Longitudinal Investigation of Marketing Communication Productivity and Shareholder Value," Journal of Marketing, 70 (October), 70–91

Mandzila, E. E. W., & Zéghal, D. (2009). Management des risques de l'entreprise : Ne prenez pas le risque de ne pas le faire! 44(237/238), 17-26.

Manfouo, S. O. (2023). L'audit interne : Une fonction au coeur de la performance de l'organisation. Editions L'Harmattan.

Mattatia, F. (2021). RGPD et droit des données personnelles. Editions Eyrolles.

Mitnick, K. (2017). The art of invisibility: The world's most famous hacker teaches you how to be safe in the age of big brother and big data. Little, Brown. https://books.google.com/books?hl=fr&lr=&id=nBBeDAAAQBAJ&oi=fnd&pg=PT6&dq=Kevin+Mitnick.+Son+livre+intitul%C3%A9+%22The+Art+of+Invisibility:+The+World%27s+Most+Famous+Hacker+Teaches+You+How+to+Be+Safe+in+the+Age+of+Big+Brother+and+Big+Data%22&ots=pXN1mnpo8m&sig=P_lgS7tA230M6CIZPjT8NSYlBDE

Moisand, D., & De Labareyre, F. G. (2009). CobiT : Pour une meilleure gouvernance des systèmes d'information. Editions Eyrolles.

Mongin, D. (2013). Les cyberattaques, armes de guerre en temps de paix. Esprit, Janvier(1), 32-49. https://doi.org/10.3917/espri.1301.0032

Mouqin, Y. (2008). Les nouvelles pratiques de l'audit de management. QSEDD, AFNOR.

Mun, J. (2012). Real options analysis: Tools and techniques for valuing strategic investments and decisions (Vol. 320). John Wiley & Sons. https://books.google.com/books?hl=fr&lr=&id=0qHsBtaJXZwC&oi=fnd&pg=PT13&dq=Johnathan+Mun+-+%22Real+Options+Analysis:+Tools+and+Techniques+for+Valuing+Strategic+Investments+and+Decisions%22&ots=6sek1d1IyX&sig=2FohRP2Q4gQ3AUeoYcSxF-jNBtI

Netwrix, P.-L. L., Country Manager France. (2024, mars 12). La certification ISO 27001 est-elle suffisante pour la conformité RGPD ? Global Security Mag Online. https://www.globalsecuritymag.com/La-certification-ISO-27001-est,20180619,79326.html

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. NIST Special Publication, 800, 181.

Nguyen, N. H. (2018). Essential Cyber Security Handbook In French : Manuel sur la cybersécurité essentielle en français. Nam H Nguyen.

Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research. Evidence-based nursing, 18(2), 34-35.

OECD. (2002). Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel. OECD Publishing.

Ouchchikh, R., Bari, A. A., & Bahjaoui, H. (2023). L'impact de la gestion des risques sur la performance financière des banques commerciales au Maroc. Revue des Études Multidisciplinaires en Sciences Économiques et Sociale, 8(2), Article 2. https://doi.org/10.48375/IMIST.PRSM/remses-v8i2.35798

Patton, M. Q. (1987). How to use qualitative methods in evaluation. Sage. https://books.google.com/books?hl=en&lr=&id=0co1ESOVJHkC&oi=fnd&pg=PA5&dq=qualitative+methods+in+evaluation&ots=wJt2EFg2E7&sig=mVJNyNOHvJhsYr0JCnf8983m9i4

Perrow, C. (1999). Normal accidents: Living with high risk technologies. Princeton university press. https://books.google.com/books?hl=fr&lr=&id=VC5hYoMw4N0C&oi=fnd&pg=PR7&dq=Charles+Perrow.+Son+livre+intitul%C3%A9+%22Normal+Accidents:+Living+with+High-Risk+Technologies&ots=MG9kbP45e8&sig=I9YTrlu4OrsjJWF7ZKCDSU1bjmA

Pesqueux, Y. (2003). Le concept de risque au magasin des curiosités. CD. https://shs.hal.science/halshs-00582808

Pickvance, C. G. (2001). Four varieties of comparative analysis. Journal of Housing and the Built Environment, 16(1), 7-28. https://doi.org/10.1023/A:1011533211521

Pomerleau, P.-L., & Lowery, D. L. (2020). The Evolution of the Threats to Canadian Financial Institutions, the Actual State of Public and Private Partnerships in Canada. In P.-L. Pomerleau & D. L. Lowery, Countering Cyber Threats to Financial Institutions (p. 47-85). Springer International Publishing. https://doi.org/10.1007/978-3-030-54054-8_4

Pompon, R. (2016). IT security risk control management: An audit preparation plan. Apress. https://books.google.com/books?hl=fr&lr=&id=sIMSDQAAQBAJ&oi=fnd&pg=PR5&dq=+Ray+Pompon+%22Cybersecurity%22&ots=mEty73gIy2&sig=fnlrdlVe53UzzwSKc5d5WDqoLTw

Protection des renseignements personnels—Commission d'accès à l'information du Québec. (2012, avril 22). https://www.cai.gouv.qc.ca/organismes/protection-des-renseignements-personnels/

Rakotomandimby, L. (s. d.). (2023). La protection des renseignements personnels du consommateur dans un système bancaire ouvert : Étude comparative entre le droit canadien et le droit québécois ainsi que le droit de l'Union européenne et le droit français.

Ramboarisata, L., De Serres, A., & Gendron, C. (2008). Gestion responsable des ressources humaines : Évaluation théorique et analyse du discours des banques canadiennes sur leur pratique: Revue internationale de psychosociologie, Vol. XIV(33), 225-258. https://doi.org/10.3917/rips.033.0225

Ramboarisata, L., Serres, A., & Gendron, C. (2006). Étude des pratiques des banques canadiennes en matière de divulgation d'information sur leur responsabilité sociale. Management et sciences sociales, 2, 75-99.

Reis, S., & Henrard, L. (2017). " La cyber-sécurité dans les institutions financières : Comment se prémunir contre le cyber-risque et développer un environnement cyber-résilient? https://dial.uclouvain.be/downloader/downloader.php?pid=thesis%3A11064&datastream=PDF_01&cover=cover-mem

Renard, J. (2017). Théorie et pratique de l'audit interne : Primé par l'IFACI. Editions Eyrolles.

Responsable de la protection des renseignements personnels—Commission d'accès à l'information du Québec. (2021, octobre 21). https://www.cai.gouv.qc.ca/espace-evolutif-modernisation-lois/thematiques/responsable-protection-renseignements-personnels/

Richard, D., Benbrahim, Z., Chabanet, D., & Perea, C. (2020). L'holacratie : Une nouvelle gouvernance tournée vers la gestion des risques ? Question(s) de management, 28(2), 131-139. https://doi.org/10.3917/qdm.202.0131

Richard, J. (2018). La divulgation de l'information protégée et les libertés économiques [PhD Thesis, Université Paris Saclay (COmUE)]. https://theses.hal.science/tel-02004294/

Richards, N. (2022). Why privacy matters. Oxford University Press. https://books.google.com/books?hl=fr&lr=&id=OARREAAAQBAJ&oi=fnd&pg=PP1&dq=Richards,+N.+(2022).+Why+privacy+matters.+Oxford+University+Press.&ots=-sGw22G8vP&sig=eUTAGl6sDcKX2s6KjRIiIqDwMPo

Rico, J.-F. D. (2020). Protection des renseignements personnels au Québec – Aperçu des modifications à la loi applicable au secteur privé.

Ruse, E., Susmanschi (badea), G., & Dăneci-Pătrău, D. (2014). Internal Audit And Risk Management. SEA - Practical Application of Science, 3, 525-531.

Sardi, A. (2002). Audit et contrôle interne bancaires. AFGES éd.

Sarens, G., & De Beelde, I. (2006). Internal auditors' perception about their role in risk managemen: A comparison between US and Belgian companies. Managerial Auditing Journal, 21(1), 63-80.

Sarrazin, C. (2019). Cybersécurité : Misez sur la prévention ! Gestion, 44(3), 78-82. https://doi.org/10.3917/riges.443.0078

Schick, P. (2007). Memento d'audit interne : Méthode de conduite d'une mission. Dunod.

Schick, P., & Lemant, O. (2001). Guide de self-audit : 184 items d'évaluation pour identifier et maîtriser les risques dans son organisation... ou créer un audit interne. Ed. d'Organisation.

Schmidt, E., & Cohen, J. (2014). The New Digital Ag: Transforming Nations, Businesses, and Our Lives. Knopf Doubleday Publishing Group.

Schmidt, E. E., & Cohen, J. (2014). The Future of Internet Freedom. New York Times, 11. https://learn.stleonards.vic.edu.au/vceeng/files/2014/05/Semester-1-2014-Practice-Exam-Year-11-VCE-English.pdf

Schneier, B. (2001). Secrets et mensonges : Sécurité numérique dans un monde en réseau. Vuibert.

Schneier, B. (2015). Data and Goliath : The hidden battles to collect your data and control your world. WW Norton & Company. https://books.google.com/books?hl=fr&lr=&id=MwF-BAAAQBAJ&oi=fnd&pg=PT6&dq=Bruce+Schneier+-+%22Data+and+Goliath:+The+Hidden+Battles+to+Collect+Your+Data+and+Control+Your+World%22&ots=Ui0E1JBaZ0&sig=eu_VKQxqWar5OtbHl5nzBMvdK2M

Serres, A., & Gendron, C. (2006). Étude des pratiques des banques canadiennes en matière de divulgation d'information sur leur responsabilité sociale. Management et sciences sociales, 2, 75-99.

Shaw, A. (2009). Data breach : From notification to prevention using PCI DSS. Colum. JL & Soc. Probs., 43, 517.

Silvestre Pinheiro, D. (2022). L'éthique de l'intelligence artificielle : Les principes et les mesures qui pourraient inspirer l'élaboration d'un cadre éthique dans l'administration publique québécoise. https://espace.enap.ca/id/eprint/351/

Simonnet, C. (2015). La gestion des risques portés par le client en banque et assurance : Comportements et éthique des acteurs [PhD Thesis, Paris, CNAM]. https://www.theses.fr/2015CNAM1020

Sinha, A., Jaiswal, A., Gupta, R., & Chaurasiya, V. K. (2011). SAS 70 to SSAE 16/ISAE 3402 : An insight into outsourcing security and process controls, and significance of new service audit standards. ISSN 1931-0285 CD ISSN 1941-9589 ONLINE, 315. https://core.ac.uk/download/pdf/67559349.pdf#page=338

Solove, D. J. (2005). A taxonomy of privacy. U. Pa. l. Rev., 154, 477.

Solove, D. J. (2010). Understanding privacy. Harvard university press. https://books.google.com/books?hl=fr&lr=&id=eSrnEAAAQBAJ&oi=fnd&pg=PT7&dq=.+Daniel+J.+Solove+-

+%22Understanding+Privacy%22&ots=MdpUiE1u0k&sig=modwdxHYlkDK7Z2S9QqmKfHO8Vo

Solove, D. J. (2022). The limitations of privacy rights. Notre Dame L. Rev., 98, 975.

Solove, D. J., & Schwartz, P. M. (2011). Privacy law fundamentals. D. Solove & P. Schwartz, PRIVACY LAW FUNDAMENTALS, International Association of Privacy Professionals. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1790262

Spence, M. (1973). Job market signaling, Quarterly Journal of Economics, 87(3), 355-374

Stross, C. (2007). Halting state (Vol. 1). Penguin. https://books.google.com/books?hl=fr&lr=&id=-t4SB9VQDI8C&oi=fnd&pg=PA1&dq=Charles+Stross+%22Halting+State%22&ots=nGLzoHbaG_&sig=7E2SmU5l8QbhZk_LIqhgS-xzE8g

Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020). Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss. JOIV: International Journal on Informatics Visualization, 4(4), 225-230.

Taillat, S., Cattaruzza, A., & Danet, D. (2023). La Cyberdéfense-2e éd. : Politique de l'espace numérique. Armand Colin. https://books.google.com/books?hl=fr&lr=&id=JMmsEAAAQBAJ&oi=fnd&pg=PT3&dq=La+cybers%C3%A9curit%C3%A9+est+un+processus+en+perp%C3%A9tuelle+surveillance+et+gestion&ots=OlHkGZ4Pi5&sig=Bh-H-xW10CCwJIKTdhWG6dBigic

Tambou, O. (2020). Manuel de droit européen de la protection des données à caractère personnel. Bruylant.

Thibodeau, M.-O. (2020). Avancées technologiques et protection de la vie privée. Bibliothèque du Parlement.

Thomas, J., O'Mara-Eves, A., & Brunton, G. (2014). Using qualitative comparative analysis (QCA) in systematic reviews of complex interventions: A worked example. Systematic Reviews, 3(1), 67. https://doi.org/10.1186/2046-4053-3-67

Trudel, P., & Benyekhlef, K. (1997). Approches et stratégies pour améliorer la protection de la vie privée dans le contexte des inforoutes. https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/71/0072.pdf

Uwamahoro, A. M. (2022). Audit interne et gouvernance des banques [PhD Thesis, Université Mouloud Mammeri]. https://ummto.dz/dspace/handle/ummto/21813

Valéau, P., & Gardody, J. (2016). La communication du journal de bord : Un complément d'information pour prouver la vraisemblance et la fiabilité des recherches qualitatives. Recherches qualitatives, 35(1), 76-100.

Venne, J.-F. (2023). Quel appétit pour le cyber-risque? Gestion, 48(2), 74-77.

Villalonga, C. (2011). Le guide du parfait auditeur interne : Réussir des audits internes qualité, sécurité, environnement à valeur ajoutée. BoD - Books on Demand France.

Watson, D. L., & Jones, A. (2013). Digital forensics processing and procedures: Meeting the requirements of ISO 17020, ISO 17025, ISO 27001 and best practice requirements. Newnes. https://books.google.com/books?hl=fr&lr=&id=P0Hwx4F8Q7cC&oi=fnd&pg=PP1&dq=l%27ISO+27001&ots=hYsS1q5XKl&sig=DGq7NNnftg1N3tvFyYdXi_gYfMo

ANNEXE 1 : TABLEAU DES NORMES DE QUALIFICATION ET DE FONCTIONNEMENT

Les normes de qualification et de fonctionnement	
Normes de qualification « Ce que sont l'audit interne et les auditeurs »	**Normes de fonctionnement. « Ce qu'ils font »**
1000 : Mission, pouvoir et responsabilité	2000 – Gestion de l'audit interne
1100 : Indépendant et objectivité	2010 – Planification
1110- Indépendance dans l'organisation	2020 – Communication et approbation
1120- Objectivité individuelle	2030 – Gestion des ressources
1130- Atteintes à l'indépendance et à l'objectivité	2040 – Règles et procédures
1200 : Compétence et conscience professionnelle	2050 – Coordination
1210- Compétence	2060 – Rapports au Conseil et à la direction générale
1220- Conscience professionnelle	2100 – Nature du travail
1230- Formation professionnelle	2110 – Management des risques
1300 : programme d'assurance et de la qualité	2120 – Contrôle
1310- Evaluation du programme qualité	2130 – Gouvernement d'entreprise
1311- Evaluations interne	2200 – Planification de la mission
1312- Evaluation externe	2201 – Considérations relatives à la planification
1320- Rapport relatifs au programme qualité	2210 – Objectifs de la mission

1330- Utilisation de la mention « conduit conformément aux normes »	2220 – Champ de la mission
1340- Indication de non-conformité	2230 – Ressources affectées à la mission
Autres Normes	2240 – Programme de travail de la mission
ISO/CEI 27002	2300 – Accomplissement de la mission
SSAE 18/ISAE 3402	2310 – Identification des informations
PCI DSS (payment Card Industry Data Sécurité Standard)	2320 – Analyse et évaluation
NIST SP 800-53	2330 – Documentation des informations
ISO/CEI 27001	2340 – Supervision de la mission
	2400 – Communication des résultats
	2410 – Contenu de la communication
	2420 – Qualité de la communication
	2421 – Erreurs et omissions
	2430 – Indication de non-conformité aux normes
	2440 – Diffusion des résultats
	2500 – Surveillance des actions de progrès
	2600 – Acceptation des risques par la direction générale

Source : Schick P., 2007, « Memento d'audit interne : Méthode de conduite d'une mission. »

ANNEXE 2 : TABLEAU 3 : LES RISQUES DE PROTECTION DE RENSEIGNEMENTS PERSONNELS DIVULGUES DE 2020 A 2022 PAR LES TRENTE-QUATRE BANQUES CANADIENNES ETUDIEES

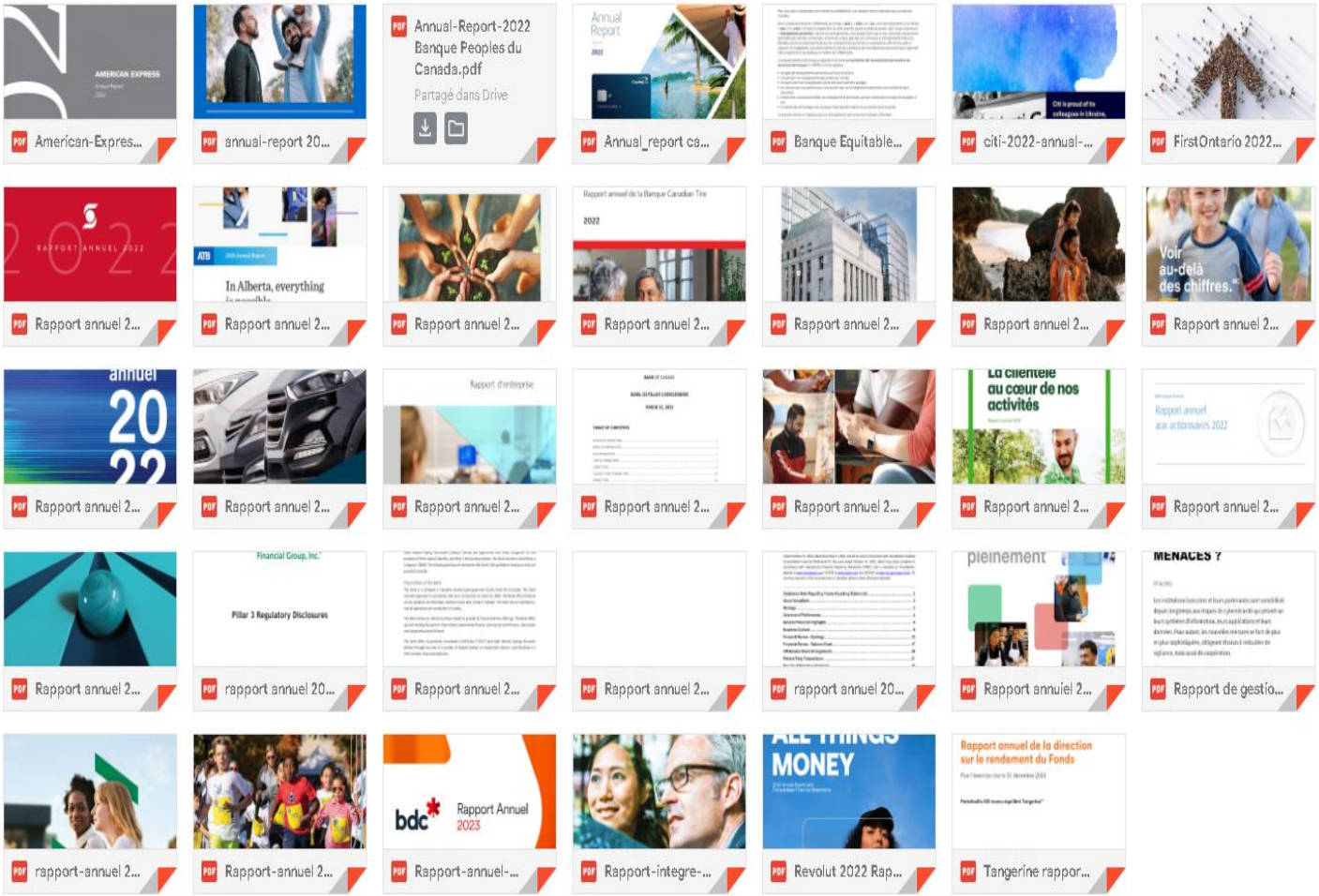
N°	Banques	Catégorie de Risque 1	Catégorie de Risque 2	Catégorie de Risque 3	Catégorie de Risque 4	Procédures mise en place
1	Laurentienne	Risques liés à la technologie, aux systèmes d'information et la cybersécurité	Risques liés à la dépendance envers la technologie et des tiers	Conjoncture économique et commerciale générale		L'identification proactive des menaces potentielles, la mise en œuvre de mesures de sécurité renforcées, la mise en place des protocoles de réponse aux incidents
2	Banque Nationale	Risques liés à la sécurité de l'information	Risques liés à la cybersécurité			Mise en place d'un cadre de gestion des risques non financiers, Renforcement de la cybersécurité et de la continuité des activités, Sensibilisation du personnel à la sécurité informatique, Collaboration avec des partenaires et utilisation d'équipes spécialisées en cybersécurité
3	Banque canadienne impériale de commerce (CIBC)	Risque lié à la technologie	Risque lié à la sécurité de l'information	Risque lié à la cybersécurité		Investissement accru dans les mécanismes de défense en cybersécurité, Mise en place d'examens du risque stratégique, d'outils technologiques et de programmes de sécurité de l'information, Surveillance constante des cybermenaces mondiales et des exigences réglementaires, Exercices de cybersécurité, protocoles d'intervention et assurance contre les cyberrisques, Evaluation périodique de l'assurance, Surveillance continue des risques et améliorations constantes des stratégies de sécurité.
4	Desjardins	Risque lié aux technologies de l'information	Risque lié à la sécurité			Allouer des fonds pour la création d'un laboratoire de cybersécurité, Suivi et conformité aux réglementations en matière de cybersécurité, Mise en place d'une gouvernance solide en matière de cybersécurité, Programmes de modernisation de renforcement de sécurité, Bureau de la sécurité Desjardins.
5	Banque du Canada	Risques liés aux technologies	Risques liés aux processus informatiques			Investissements dans les technologies et les processus informatiques, Test de la capacité de réponse aux cyberattaques et de reprise des activités, Collaboration avec des partenaires externes, Recrutement et fidélisation d'employés qualifiés et diversifiés dans le domaine de la cybercriminalité
6	Banque Scotia	Risque lié aux tiers, à la cybersécurité	Risques liés aux technologies de l'information (TI)	Risque lié à la sécurité des données	Risque de conformité	Investissement dans la technologie, l'expertise et les assurances, Renforcement du processus d'évaluation et de surveillance des risques associés aux fournisseurs tiers, Mise en place d'un comité de gestion du risque et d'une équipe de gestion des risques, Approche collaborative pour la gestion des risques liés aux données.
7	Banque de Montréal	Risque lié à la cybersécurité et	Risque lié à la dépendance envers la technologie	Risques liés à la sécurité de l'information et à la vie privée	Risque lié à la sécurité infonuagique	Investissements dans l'unité crime financier et l'infrastructure technologique, Améliorations continues des capacités technologiques, Innovation technologique et utilisation des données avancées et de l'intelligence artificielle
8	Banque TD Canada Trust	Risque lié à la technologie	Risque lié aux cyberrisques	Risque lié aux prestataires de services indépendant		Surveillance, gestion et amélioration constante de la cybersécurité, Mise en place de sous-comité dédié à la cybersécurité, Cadre de gestion du risque opérationnel et programmes de cybersécurité, Bureau de la gouvernance des données de l'entreprise
9	Banque Alterna	Risque lié à la technologie				Planification avant-gardiste et investissement dans les nouvelles technologies, Amélioration constante des capacités de défense, Formation des employés et partage d'informations, Fourniture de conseils et d'astuces aux clients
10	Banque Comerica	Risque lié aux technologies de l'information	Risque lié à la sécurité	Risque lié à la cybersécurité		Gestion des risques liés à l'information et à la cybersécurité, Maintenance et sécurisation des systèmes informatiques, Adaptation au travail à distance, Gestion des conséquences des incidents
11	Banque JP Morgan Canada	Risques liés à la sécurité de l'information	Risques liés à la cybersécurité			Divers programmes de gestion des risques opérationnels, Système de gestion des risques opérationnels, Protection des activités contre les cyberincidents

12	HSBC Banque Canada	Risque lié aux tiers	Risques liés à la cybersécurité	Risques liés aux technologies de l'information		Investissements massifs dans les contrôles commerciaux et techniques, Évaluation continue des menaces, Politiques et systèmes de gestion exemplaires, Sensibilisation et formation du personnel
13	Banque Royale du Canada	Risques liés aux changements de la réglementation sur le numérique, les données, la technologie	Risque lié à la gestion des données, à la cybersécurité	Risque lié aux technologies de l'information	Risque lié aux tierces parties et à la confidentialité	Mise en place de gestion du risque lié aux technologies de l'information, Gestion du risque lié à la cybersécurité, Renforcement du cadre de gestion du risque lié à la cybersécurité, Gestion du risque lié à la confidentialité, Gestion du risque lié à la confidentialité
14	Revolut	Risque de cybersécurité	Risque lié à la sécurité des données			Mise en place de gestion des cybermenaces, Sécurité avancée des données et des systèmes, Résilience opérationnelle
15	Coast Capital	Risques liés aux technologies de l'information (TI) et	Risques liés aux cyber-risques,	Risques liés aux tiers		Évaluation de la sécurité des fournisseurs, Surveillance continue des fournisseurs, Adaptation constante, Conformité réglementaire
16	TangerineMD	Risques liés à la révolution technologique	Risques liés aux modifications de la loi et de la réglementation			Méfiance à l'égard des logiciels, Protection des mots de passe, Authentification des achats en ligne, Protection de l'identité
17	FirstOntario	Risque lié aux technologies de l'information	Risque lié à la cybersécurité	Risque lié à la gestion des données et à la confidentialié	Risque lié à la technologie	Précautions en ligne, Mots de passe forts, Sensibilisation au phishing, Surveillance régulière et alertes, Signalement des fraudes
18	Banque Équitable (EQ)	Risque lié aux changements de la réglementation sur le numérique, les données, la technologie et la cybersécurité,	Risque lié à la gestion des données et à la confidentialité	Risque lié aux technologies de l'information et à la cybersécurité	Risque aux tierces parties	Entente de confidentialité, Responsabilité des renseignements personnels, Loi sur la protection des renseignements personnels, Collecte de renseignements personnels, Utilisation des renseignements personnels
19	Banque Manuvie Canada	Risque lié à la technologie et	Risque lié à la sécurité informatique			Fonction de gestion des risques liés à la technologie, Programme d'information et de cybersécurité, Formation de sensibilisation

20	Services financiers Le choix du Président	Incapacité de l'infrastructure de TI	Occurrence d'atteintes à la sécurité de renseignements internes ou externes	Attaques par déni de service, virus et vers informatiques		Formation des collègues sur la sécurité, Contrôles et tests réguliers, Maintenance des systèmes de protection des données, Plans de reprise après sinistre, Investissements stratégiques pour atténuer les risques de cybermenaces, Plans de reprise après sinistre, Procédures, protocoles et normes de sécurité pour les tiers fournisseurs de services
21	Canadian Western Bank	Risques liés aux données, dépendance à l'égard de la connectivité à distance, des plateformes numériques publiques	Recours accru à des fournisseurs de services tiers	Risques liés à l'adoption de technologies émergentes		Identification des points de défaillance potentiels, Conception et mise en œuvre efficace de technologies, processus et outils appropriés, Mise en œuvre d'une approche collaborative et holistique de la gestion des risques liés aux données, Utilisation d'un cadre de gestion des risques liés aux tiers
22	Banque de développement du Canada	Vulnérabilités ou faiblesses des contrôles informatiques	Risque lié aux défaillances des activités technologiques	Risque lié à la défaillance de tiers	Risque lié aux données	Mise en place des politiques et des directives, Investissement dans son infrastructure technologique, Adoption des principes stricts en matière d'approvisionnement et de passation de contrats, Programme de formation
23	Citizens Bank of Canada	Risques liés à la défaillance des systèmes opérationnels de sécurité,	Risques liés à la défaillance des infrastructures opérationnels de sécurité	Risques liés à la violation des systèmes des fournisseurs tiers		Approche intégrée de gestion des risques, Gouvernance et surveillance des risques Comités de risque spécifiques, Rapport régulier sur la situation des risques
24	General Bank of Canada	Risque lié à la technologie	Risque lié aux données	Risque lié aux tiers		Mise en place de modèle des trois lignes de défense, Mis en place d'un programme de gestion des risques liés aux tiers
25	Versa bank	Risque lié à la technologie				Mise en place des services de cybersécurité et des opérations de développement de technologies bancaires et financières, Evaluation continuelle des données et informations
26	Banque Peoples du Canada	Risque lié aux tiers,	Risque lié à la technologie informatique	Risques et des cyberrisques		Gestion des risques informatiques et des cyberrisques, Information et sensibilisation, Participation active aux associations industrielles
27	Banque RFA du Canada	Risque découlant de l'utilisation d'une technologie obsolète	Défaut de protéger les informations	Expositions aux risques d'un partenaire commercial		Mise en place d'un cadre de gestion des risques opérationnels (GRE)
28	Banque Motus	Risque lié aux technologies	Risque lié a à la sécurité de l'information			Réduction de la complexité des systèmes, Protection des informations sensibles, Investissements dans la technologie, Réduction de la complexité des systèmes
29	Banque Rogers	Risques liés à la cybersécurité				Programme de sécurité de l'information et de cybersécurité, Formations de sensibilisation à la sécurité, Politiques et procédures de sécurité, Surveillance des risques liés à la cybersécurité, Assurance cybersécurité, Confidentialité des données
30	Capital One	Risque lié aux données	Risque lié à la technologie			Gestion du risque opérationnel, Système de gouvernance, de gestion des risques et de conformité, Politiques, normes et contrôles en matière de gestion des risques opérationnels, Rapports sur les risques opérationnels
31	Canada-Société Générale	Défaillance des systèmes IT				Sécurité du système d'information, Protection des clients via OPPENS, Sensibilisation et Formation en cybersécurité

32	Caisses Populaires Acadiennes	Risque de cybersécurité	Risque de sécurité des données			Mise en place des politiques, directives, procédures, système informatique sécurisé, règle, normes, plan de continuité des affaires et contrôle interne
33	Alberta Treasury Branches	Manque de formation/ sensibilisation, de vulnérabilités des fournisseurs/de la chaîne d'approvision-nement	Conformité inefficace des contrôles de cybersécurité	Conformité inefficace de la concentration des données et des analyses associées	Manque de ressources/ d'investissement, de la gestion des dépendances externes	Identification du risque de cybersécurité, Approche interdisciplinaire, Gestion des risques de cybersécurité durable, Investissements dans la cybersécurité, Renforcement de la résilience face aux cyberattaques
34	Citi Canada	Risque de cybersécurité				Stratégie axée sur les menaces, Gestion du risque en trois lignes de défense ; Surveillance et évaluation continue, Contrôle interne et assurance indépendante, Gouvernance du conseil d'administration

ANNEXE 3 : LES RAPPORTS ANNUELS DES 34 INSTITUTIONS FINANCIERES DU CANADA



le Choix du Président

Desjardins

BMO

CIBC

BANQUE LAURENTIENNE

RBC

TD

Banque Scotia

HSBC