Université de Montréal

Mieux vaut prévenir **ET** guérir : la réaction du public envers la posture de cyber-résilience des entreprises après un vol de données

Par
Traian Toma

École de criminologie
Faculté des Arts et des Sciences

Mémoire présenté en vue de l'obtention du grade de Maîtrise ès sciences en criminologie, option mémoire

Août 2021

Université de Montréal
École de criminologie, Faculté des arts et des sciences

Ce mémoire intitulé

Mieux vaut prévenir ET guérir : la réaction du public envers la posture de cyber-résilience des entreprises après un vol de données

Présenté par

Traian Toma

A été évalué par un jury composé des personnes suivantes

Étienne Blais
président-rapporteur

David Décary-Hétu
directeur de recherche

Benoît Dupont
codirecteur

Isabelle Daignault
membre du jury

RÉSUMÉ

Les recherches montrent que les clients ne prennent guère de mesures pour se protéger des crimes qui peuvent découler d'une brèche de renseignements confidentiels au sein d'une entreprise. Plutôt, ils considèrent que la firme — hébergeuse de leurs informations personnelles — a la responsabilité absolue en matière de la confidentialité continue de leurs données. Les commerces qui manquent de protéger adéquatement les informations clients risquent en contrepartie de subir des torts réputationnels ruineux. Cela dit, peu de travaux explicatifs sont effectués sur la résilience des entreprises face à la réaction négative du public après un vol de données. Ainsi, une étude expérimentale basée sur des vignettes de cas a été menée à l'aide du modèle de la victime « idéale ». Les mises en situation illustrent : (1) une entreprise victime décrite comme ayant une forte posture de cyber-résilience ; (2) une entreprise victime décrite comme ayant une faible posture de cyber-résilience. Un échantillon final de 664 participants a été aléatoirement affecté à l'une des deux conditions expérimentales principales. Les résultats révèlent que, comparativement à une faible posture de cyber-résilience, une bonne posture de cyber-résilience minimise les attitudes négatives des clients et favorise leurs intentions comportementales positives vis-à-vis la firme victime. À la lumière de ces résultats, la cyber-résilience, qui a principalement fait l'objet d'une attention conceptuelle, acquiert un fondement empirique. Par ailleurs, ce projet de recherche contribue plus généralement au développement de la victimologie des entreprises.

Mots-clés : Cybersécurité, Cyber-résilience, Brèche de données, Réputation, Réaction sociale, Gestion des risques, Communication de crise, Faute de la victime, Victime idéale, Vignettes de cas

ABSTRACT

Research shows that customers take few measures to protect themselves from crimes that may follow data theft at a business. They rather consider that the firm—the host of their personal information—holds exclusive responsibility over the continued confidentiality of their data. Companies that fail to properly secure customer information may, in return, risk experiencing ruinous reputational harm. That said, little explanatory research is done on the resilience of businesses to negative public reaction after data theft. Consequently, a vignette-based experimental study was conducted using the "ideal" victim model. The scenarios feature: (1) a breached business described as having a strong cyber-resilience posture; (2) a breached business described as having a weak cyber-resilience posture. A final sample of 664 participants was randomly assigned to one of the two main experimental conditions. Results reveal that compared to a weak cyber-resilience posture, a good cyber-resilience posture minimizes negative customer attitudes and promotes positive customer behavioural intentions towards the company. Considering these results, cyber-resilience, which has mainly received conceptual attention, gains empirical support. Furthermore, this research project contributes more broadly to the evolution of the victimology of businesses.

Keywords: Cybersecurity, Cyber-resilience, Data breach, Reputation, Social reaction, Risk management, Crisis communication, Victim blaming, Ideal victim, Vignettes

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES ABRÉVIATIONS

- LPRPDE : Loi sur la protection des renseignements personnels et les documents électroniques
- CID : Confidentialité-Intégrité-Disponibilité
- CPVPC : Commissariat à la protection de la vie privée
- PME : Petites et moyennes entreprises
- NCSA : National Cyber Security Alliance
- CVE : Common Vulnerabilities and Exposures
- NIST : National Institute for Standards and Technology
- ISO : International Organization for Standardization

REMERCIEMENTS

J’aimerais en premier lieu remercier mes directeurs de recherche David Décary-Hétu et Benoît Dupont pour leur disponibilité de même que pour leur appui continu à travers l’élaboration et la rédaction du projet de mémoire. Merci à Benoît, Fyscillia et à l’ensemble de la Chaire de recherche en prévention de la cybercriminalité pour le financement de mes études ainsi que pour les diverses opportunités professionnelles. Grâce à vous, j’ai pu développer mes compétences en recherche et tisser des liens avec plusieurs experts de la cybersécurité. Merci d’ailleurs à Julien Hivon et à toute l’équipe de la sécurité des accès chez Desjardins pour m’avoir accueilli l’été passé en tant qu’étudiant-chercheur en matière de cybersécurité. Merci aussi à l’École de Criminologie de l’Université de Montréal pour son soutien financier.

Sur le plan personnel, merci à toute ma famille pour son appui émotionnel lors de la rédaction de mon projet de mémoire, spécialement lors de ces temps tumultueux de pandémie. Enfin, merci à Matthieu pour les nombreux discussions et débats stimulants entretenus en ligne pendant cette longue période de confinement.

INTRODUCTION

Alors que la grande majorité des entreprises canadiennes utilisent déjà les technologies numériques pour mener à bien leurs opérations quotidiennes (Bilodeau et al., 2019), le marché contemporain semble maintenant s'introduire dans une quatrième révolution industrielle, l'Industrie 4.0 (Schwab, 2016). La collecte, le stockage et l'analyse des données, le cœur de l'Industrie 4.0, permettent aux entreprises d'authentifier leurs clients (Freedman, 2020) et d'offrir une expérience client personnalisée de même que conviviale sur leurs plateformes (Chen et al., 2012). Les commerces s'imprégnant d'une culture dite *data-driven* se démarquent d'ailleurs de la concurrence parce qu'elles peuvent prendre des décisions entrepreneuriales rapides et éclairées qui comblent les nouvelles attentes des consommateurs (Vassakis et al., 2018). Ainsi, certaines sources indiquent que 72 à 75 % des clients ont davantage tendance à fréquenter une entreprise si celle-ci est capable de fournir des recommandations de produits à partir de leurs besoins et préférences (Gladly, 2019 ; Salesforce, 2018). La plupart croient également qu'il est plus facile que jamais de changer de service, et plus de la moitié des consommateurs n'ont pas hésité à le faire lorsqu'ils ont jugé insatisfaisante l'expérience client (Salesforce, 2018).

Pendant que les entreprises désirant avoir un avantage concurrentiel sur le marché sont incitées à participer dans la course aux données clients, le stockage de plus en plus massif de renseignements personnels pourrait malencontreusement impliquer un vaste montant de victimes dans l'éventualité où les informations en question tombent entre les mains de contrevenants motivés (Rosati et al., 2019). Par exemple, durant le vol de données notoire chez Yahoo en 2013, des acteurs malveillants se sont emparés des noms, dates de naissance, pairs d'adresses courriel/mots de passe ainsi que les réponses aux questions secrètes d'un record mondial de trois milliards de comptes utilisateur (Swinhoe, 2020). Or, ce n'est pas tant le vol des informations en soi qui pose un problème aux parties prenantes que les crimes qui en découlent, notamment la fraude à l'identité (Sullivan et Maniff, 2016), autrement dit l'utilisation de renseignements volés en vue de commettre un autre crime (comme soumettre des demandes de prêts, acheter des biens et services ou encore obtenir des prestations du gouvernement sous le nom d'une autre personne) (Centre antifraude du Canada, 2021). De même, les particuliers peuvent être assujettis à des campagnes d'hameçonnage personnalisées qui cherchent à recueillir davantage d'informations personnelles pour favoriser la fraude à l'identité (Trend Micro, 2017). Dans une nouvelle époque où les fuites de données comme celle au sein de Desjardins ou de Capital One font les manchettes

(CPVPC, 2019), les craintes liées à la compromission des renseignements et à la fraude à l'identité sont devenues courantes parmi les particuliers (Ponemon, 2014 ; Salesforce, 2018). Piquero et *al.* (2011) révèlent même une opinion publique favorable à des taxes additionnelles pour la prévention de la fraude à l'identité.

En raison des préoccupations populaires liées aux brèches d'informations personnelles, de nombreux pays industrialisés, dont le Canada (CPVPC, 2018), ont mis en vigueur des dispositions juridiques qui obligent les organisations à aviser leurs parties prenantes des brèches de données lorsqu'elles surviennent en leur sein (Zou et Schaub, 2019). Ces lois ont comme premier objectif d'informer les particuliers des risques encourus et de les encourager à entamer les démarches nécessaires pour se protéger des préjudices possibles (Ablon et al., 2016). Dans un deuxième temps, ces lois espèrent pousser les entreprises à investir davantage dans la protection des données, si ce n'est pour éviter les dommages réputationnels causés par l'exposition publique d'une faille de sécurité (Ablon et al., 2016 ; Laube et Böhme, 2016). La réputation, c'est-à-dire l'évaluation agrégée que font les parties prenantes sur la capacité d'une entreprise à combler leurs attentes (Wartick, 1992), est une ressource intangible que les firmes convoitent parce qu'elle représente un atout concurrentiel sur le marché (Boyd et al., 2010). Gatzert (2015) conclut dans sa revue systématique qu'elle favorise la fidélité des clients, les intentions d'achat et les recommandations auprès des pairs. De même, les fournisseurs et les investisseurs sont plus enclins à faire affaire avec une organisation réputée.

L'étude ci-présente explore la réaction du public à l'égard des entreprises touchées par un vol de données. Plusieurs auteurs ont souligné ici la curieuse situation des firmes : même si elles sont techniquement les victimes d'une cyberattaque, elles peuvent entrer dans la ligne de mire de leurs parties prenantes, car ces dernières s'attendent à ce que les informations qu'elles ont confiées soient protégées de toute intrusion (Bentley et al., 2018 ; Choi et al., 2016 ; Malhotra et Malhotra, 2011). Ces dégâts de nature réputationnelle affectent ultimement les revenus ainsi que la croissance des commerces concernés et peuvent même représenter une menace existentielle pour ces derniers s'ils ne sont pas maîtrisés (Knight et Nurse, 2020 ; The Economist Intelligence Unit, 2016 ; Verhagen et al., 2013). À l'aide du modèle de la victime « idéale » adaptée par Hopkins (2016) pour les entreprises, ce projet de recherche examine la responsabilisation des entreprises

victimes de vol de données. La faute fait partie intégrante du concept de la victime « idéale ». Autrement dit, la notion sous-entend que certaines victimes seront critiquées plus que d'autres en vertu des actions ou l'absence d'actions liées à leur victimisation (Cross et al., 2019). Comme il sera détaillé prochainement, le public pourrait responsabiliser une entreprise pour un vol d'informations à cause de ses mesures de prévention lacunaires, certes, mais aussi en raison de ses faibles capacités de réponse à l'incident (Syed, 2019). À la lumière de ces idées préliminaires, l'étude détermine si la réaction du public envers une firme touchée par un vol de données change selon sa posture de cyber-résilience, c'est-à-dire sa « capacité d'une organisation à limiter les dommages causés par les cyberperturbations, à maintenir ses activités essentielles et à retrouver rapidement son fonctionnement normal à la suite d'un cyberincident » (Bryson, 2018, p. 1).

Même si plusieurs rapports dévoilent que les dommages réputationnels constituent la préoccupation principale des hauts dirigeants d'entreprises à la suite d'un vol d'informations confidentielles (Ponemon, 2017 ; The Economist Intelligence Unit, 2016), la cyber-résilience demeure dans sa phase conceptuelle (Dupont et al., 2020) et il existe conséquemment peu de travaux explicatifs sur les façons de rebondir de la réaction du public après un tel incident. En plus de contribuer à la victimologie des entreprises, un sous-domaine niche de la criminologie (Hopkins, 2016), l'étude fournit aux organisations privées des pistes envisageables pour assurer la cyber-résilience face aux dommages réputationnels après un vol de renseignements personnels.

Dans le cadre du modèle de Hopkins (2016), une démarche expérimentale a été employée, où des vignettes de cas ont été distribuées de façon aléatoire aux participants de l'étude. En vertu du soutien empirique qu'elles ont reçu, trois des six dimensions de l'entreprise victime « idéale » ont été incluses dans les vignettes de cas : la qualité « fragile », « respectable » et « irréprochable » de la victime (Lewis et al., 2019). À partir des idées de Hopkins (2016), une entreprise devrait fortement limiter la réaction négative du public après un vol de données si elle est d'abord une petite entreprise (victime « fragile ») (Malhotra et Malhotra, 2011 ; Rosati et al., 2019). Le crime doit aussi susciter une indignation morale en sa faveur (victime « respectable »). Les recherches montrent que le public s'indigne peu contre l'entreprise si le vol de données est décrit comme ayant affecté un nombre limité de personnes et s'il ne concerne que des données non financières (Garg et al., 2003 ; Gatzlaff et McCullough, 2010 ; Kamiya et al., 2020 ; Malhotra et Malhotra,

2011 ; Miller et Angelis, 2018 ; Morse et al., 2011 ; Romanosky et al., 2014 ; Tweneboah-Kodua et al., 2018 ; Tweneboah-Kodua et al., 2020). Enfin, la firme victime doit (3) avoir des mesures de prévention et de réponse robustes (contrôles préventifs de base ; chiffrement des données ; avis immédiat, transparent et exprimant le regret ; ouverture de dialogue avec le public), c'est-à-dire une forte posture de cyber-résilience (victime « irréprochable ») (Choi et al., 2016 ; Gwebu et al., 2018 ; Muzatko et Bansal, 2018 ; Novak et Vilceanu, 2019 ; Ponemon, 2017 ; Romanosky et al., 2014 ; Rosati et al., 2019 ; Syed, 2019 ; Syed et Dhillon, 2015).

Les dimensions à l'étude ont été dichotomisées pour donner lieu à 8 vignettes de cas. Celles-ci mettent en vedette soit : (1) une entreprise victime de vol de données avec une forte posture de cyber-résilience ; (2) une entreprise victime de vol de données avec une faible posture de cyber-résilience. De même, l'entreprise est soit de petite ou de grande taille. Enfin, elle a soit subi un vol de données affectant les données financières d'un grand nombre de clients, ou un vol ne touchant que les données non financières d'un nombre limité de clients. Les participants lisent une des huit mises en situation qui leur a été aléatoirement affectée. Après la lecture de leur vignette de cas, les participants répondent à un sondage, sur lequel ils expriment leurs attitudes et leurs intentions comportementales à l'égard de la firme victime en question. L'étude tente d'expliquer l'impact d'une posture de cyber-résilience sur les (1) attitudes et les (2) intentions comportementales du public vis-à-vis les entreprises touchées par un vol de données. Elle cherche aussi à déterminer l'association entre ces attitudes et ces intentions comportementales pour voir si les dégâts réputationnels de l'incident sont liés à des répercussions économiques et donc à des implications pour la résilience d'une entreprise dans le contexte d'un vol de données (Knight et Nurse, 2020).

Ce document est divisé de la façon suivante. Le premier chapitre effectue un survol des enjeux liés aux vols d'informations confidentielles et définit les concepts-clés de l'étude. Le deuxième chapitre aborde en détail les démarches méthodologiques employées dans le projet de recherche ci-présent. Les chapitres trois et quatre présentent et discutent respectivement des résultats de l'expérience. Le projet de mémoire se conclut avec les limites de l'étude et des pistes de recherches futures.

CHAPITRE 1 — REVUE DE LITTÉRATURE

Une mise en contexte des vols de données

Conformément à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) au Canada (CPVPC, 2018), une brèche de données personnelles peut être définie de la façon suivante : « communication non autorisée ou perte de renseignements personnels, ou accès non autorisé à ceux-ci, par suite d'une atteinte aux mesures de sécurité d'une organisation […] ou du fait que ces mesures n'ont pas été mises en place ». Les brèches de données compromettent notamment la dimension « confidentialité » de la triade Confidentialité-Intégrité-Disponibilité (CID) de la cybersécurité (Andoh-Baidoo et al., 2010), car ce ne sont plus exclusivement les individus autorisés qui ont accès aux informations en question. Des types notoires de renseignements personnels illégitimement divulgués incluent les informations de cartes de crédit ou de débit, les comptes financiers, les identités émises par le gouvernement (passeports, permis de conduire, etc.), les numéros d'assurance sociale et les mots de passe (Privacy Rights Clearinghouse, 2019).

Un total mondial de 27 milliards de dossiers a été exposé durant la première moitié de 2020, une différence de plus de 12 milliards, lorsque comparée à l'entièreté de 2019 (RiskBased Security, 2020). Les chances pour une organisation de subir une compromission de renseignements continuent quant à elles de grimper chaque année (Ponemon, 2019). Au Canada, le Commissariat à la protection de la vie privée (CPVPC, 2019) a reçu 680 rapports de brèches d'informations entre les années 2018-2019, avec le nombre de Canadiens affectés dépassant les 28 millions. Bref, il semble qu'il ne soit dorénavant qu'une question de temps avant qu'un particulier soit personnellement touché par une fuite de données (Olmstead et Smith, 2017 ; Ponemon, 2014).

La définition fournie par la LPRPDE (CPVPC, 2018) laisse présager que les brèches d'informations peuvent être de nature accidentelle ou criminelle. En vue d'examiner le statut de victime des entreprises, l'étude ci-présente se focalise sur le second type, c'est-à-dire l'accès frauduleux à des données informatiques, comme indiqué dans l'article 342.1 du Code criminel canadien (Gouvernement du Canada, 2020), et constituant d'ailleurs environ 66 % des cas au Canada selon le CPVPC (2019). Surtout motivés par l'appât du gain financier, la majorité des délinquants parviennent à compromettre les bases de données confidentielles des entreprises grâce à l'abus d'identifiants obtenus de façon illicite (Verizon, 2021). Les identifiants en question sont

principalement capturés par l'entremise de campagnes d'hameçonnage (Verizon, 2021). Le cybercriminel transmet un message (typiquement un courriel) à l'apparence légitime afin de convaincre un employé avec des privilèges d'accès de lui divulguer les identifiants nécessaires à l'accès frauduleux des données personnelles emmagasinées par l'entreprise cible. Certains courriels malveillants incluront dans leur message des logiciels malveillants pour automatiser et faciliter le vol des identifiants.

Les particuliers, victimes ultimes des vols de données

Bien que les cybercriminels attaquent l'infrastructure des organisations pour s'emparer des données personnelles stockées, celles-ci se rapportent aux particuliers et ce sont ces derniers qui risquent alors de subir les préjudices subséquents (Sullivan et Maniff, 2016). La fraude à l'identité est un crime symbolisant, selon les détenus interviewés par Copes et Vieraitis (2009), une façon simple de rentabiliser les renseignements mal acquis. En revanche, il est devenu difficile pour les voleurs d'informations personnelles de tirer pleinement profit des données à fur et à mesure que le montant de dossiers compromis par brèche s'est accru, ce qui a mené à la prolifération de marchés illicites en ligne pour les renseignements confidentiels (Steel, 2019). Ces plateformes, sur lesquelles se connectent des cybercriminels de toutes les régions du monde, marchandent des masses de données volées, et ce, pour un prix modique (Holt et Lampke, 2010). Le montant d'un numéro d'assurance sociale volé est de 1 $, alors qu'un numéro de carte de crédit ou de débit vaut dans les alentours de 15 $ (KeeperSecurity, 2020 ; Stack, 2017). Un permis de conduire se vend à 20 $ et les combinaisons de courriels/mots de passe valent entre 0,70 $ à 2,30 $. La valeur d'un compte bancaire volé dépend quant à elle au montant d'argent stocké à l'intérieur (Madarie et al., 2019). Un compte avec 2000 $ ou moins peut valoir 100 $ alors qu'un compte avec 15 000 $ ou plus peut se vendre à 1000 $ (KeeperSecurity, 2020). Enfin, un fraudeur qui souhaite lancer des campagnes d'hameçonnage peut obtenir pour 400 $ la liste de 3 millions d'adresses courriel, sinon 30 millions d'adresses courriel s'il est prêt à verser 1500 $ (Holt et Lampke, 2010).

Une grande demande subsiste pour les données dérobées parce qu'elles présentent de grandes opportunités criminelles pour les acheteurs, et ce, sans le besoin d'approcher une victime directement (Holt et Lampke, 2010 ; Peretti, 2009). Par exemple, Holt et *al.* (2016) concluent que les revenus totaux peuvent facilement varier des centaines de milliers aux millions de dollars pour

les acheteurs d'informations de crédit. Les *fullz*, c'est-à-dire les gammes complètes d'informations par rapport à un compte utilisateur, sont spécialement populaires parce qu'ils facilitent davantage la fraude à l'identité (Holt et Lampke, 2010 ; Stack, 2017). Bref, la fraude à l'identité continue à grimper au Canada et sa fréquence contribue à l'augmentation de l'indice de gravité de la criminalité non-violente dans plusieurs régions du pays, comme à la Nouvelle-Écosse ou au Nouveau-Brunswick (Moreau, 2021).

Les individus très actifs dans le *e-commerce* sont spécialement à risque de la fraude à l'identité dans le contexte des fuites d'informations personnelles simplement parce qu'ils ont davantage tendance à divulguer leurs données personnelles à un grand nombre d'entreprises, ce qui augmente en conséquence leur exposition au cas où l'une de ces firmes subit une brèche en son sein (Burnes et al., 2020 ; Reyns et Henson, 2016). Ainsi, l'âge, le revenu, être de race blanche, ainsi que le niveau d'éducation sont des facteurs démographiques positivement associés à la victimisation de la fraude à l'identité parce qu'ils prédisent justement le niveau de revenu disponible nécessaire pour participer activement dans le *e-commerce* (Burnes et al., 2020).

Les répercussions de la fraude à l'identité sur les particuliers impliquent plus la détresse physique (comme les troubles de sommeil) et émotionnelle (comme l'anxiété) que les pertes économiques (Golladay et Holtfreter, 2017 ; Shay et al., 2014 ; Zaiss et al., 2019). La cybercriminalité ne coûte après tout que quelques dollars par victime (Anderson et al., 2019) et ces dernières sont typiquement remboursées par les banques ainsi que par les sociétés de cartes de crédit. C'est le processus ardu de restauration des dossiers qui explique notamment les conséquences (Whitson et Haggerty, 2008). Les autorités s'attendent à ce que les victimes consacrent plusieurs heures de leurs journées pour prouver leur innocence aux institutions financières, sous peine d'être tenues responsables des transactions frauduleuses. La victimisation répétée exacerbe la gravité de ces préjudices, mais le niveau d'éducation de même que le revenu l'atténuent (Burnes et al., 2020). Même s'ils prédisent la victimisation de fraude à l'identité, ce sont les indicateurs d'un filet de sécurité financière et les implications économiques possibles de la fraude à l'identité ne percutent donc pas autant ces individus que les personnes en situation de précarité financière (Burnes et al., 2020 ; Golladay et Holtfreter, 2017).

Les particuliers et la protection contre la fraude à l'identité, un « privacy paradox » ?

Le discours entretenu sur la prévention de la fraude à l'identité est singulier parce que la somme des solutions recommandées repose sur les épaules des individus au lieu de celles des autorités policières et des régulateurs (Ylang, 2020). Par ailleurs, le criminel en soi et sa poursuite semblent absents des discussions, donc l'attention est portée sur la victime potentielle ainsi que des démarches qu'elle peut emprunter pour gérer adéquatement les risques (Whitson et Haggerty, 2008). Ces solutions de protection individuelle contre la fraude à l'identité concernent d'une part les technologies de l'information (comme le changement de mots de passe ou l'usage d'un logiciel de sécurité), mais elles peuvent aussi impliquer la vigie des transactions bancaires ou encore l'abonnement à des services de surveillance du crédit (Lai et al., 2012 ; Ylang, 2020).

Afin de sensibiliser les particuliers à la fraude à l'identité et les inciter à se protéger des préjudices, de nombreux pays ont adopté des lois qui obligent les organisations à déclarer publiquement les brèches de données en leur sein. L'impact de ces lois sur l'adoption individuelle de mesures de protection contre la fraude à l'identité reste cependant peu fondé. D'une part, Romanosky (2011) conclut qu'elles sont efficaces après avoir examiné l'éclat desdites lois aux États-Unis. En contrepartie, Sullivan et Maniff (2016) ajoutent que la façon dont ces lois sont formulées peut tant aider que nuire à la prise de précautions contre la fraude à l'identité. Par exemple, les lois qui limitent les pénalités découlant des procès civils après une déclaration publique inviteraient une plus grande transparence de la part des entreprises, et les parties prenantes pourraient se voir ainsi mieux habilitées à entamer des démarches de protection. En revanche, les régions n'obligeant l'avis public des brèches de données que lorsqu'elles seraient préjudiciables, comme c'est d'ailleurs le cas au Canada (CPVPC, 2018), entraveraient à la sécurité des particuliers (Sullivan et Maniff, 2016). Selon les auteurs, l'entreprise ayant détecté la fuite de renseignements pourrait mal interpréter ses dangers et décider de ne pas outiller le public avec des informations qui auraient pu autrement encourager l'adoption de mesures de sécurité. Cela dit, ces études utilisent le taux de fraude à l'identité comme proxy pour en arriver à leurs résultats, avec la supposition qu'une baisse du taux de fraude à l'identité après la mise en œuvre de la déclaration obligatoire des fuites d'informations signifie une meilleure prise de précautions chez les particuliers dans une région donnée.

Examiner directement les habitudes des clients révèle que même s'ils sont touchés par une fuite de renseignements, les particuliers sont peu motivés à se protéger de la fraude à l'identité, et ce, malgré les vives inquiétudes suscitées par l'incident (Bhagavatula et al., 2020 ; Golla et al., 2018 ; LastPass, 2020 ; Ponemon, 2014 ; Zou et al., 2018). Ce phénomène semble à première vue renvoyer à la notion du *privacy paradox* : même si les utilisateurs affirment chérir l'intégrité de leur vie privée, leurs comportements de sécurité ne se conformeront pas nécessairement à leurs convictions (Barnes, 2006). Les clients ont plutôt tendance à reléguer ce fardeau aux hébergeurs de leurs données confidentielles, c'est-à-dire les commerces (Gemalto, 2018 ; Ping Identity, 2019). La majorité des particuliers croient que les firmes ne prennent pas ce devoir sérieusement et que ces dernières devraient investir davantage dans la protection des données si elles espèrent préserver la loyauté de leur clientèle (Gemalto, 2018). Certains auteurs vont cependant dire que cette manière de penser réfute justement l'argument du *privacy paradox*, car même si les particuliers n'adoptent pas eux-mêmes des comportements de sécurité, ils récompensent ou punissent les entités pour lesquels ils croient responsables de la protection des données (Martin et al., 2020). Ainsi, Berezina et *al*. (2012) montrent que les clients ont davantage tendance à revisiter un hôtel et de le recommander à leurs pairs s'ils apprennent que l'établissement a passé un audit exhaustif de sécurité à l'égard de leurs renseignements personnels. Par surcroît, les firmes risquent de subir une réaction négative du public si elles manquent de prévenir les vols de données parce qu'elles ont brimé les attentes des parties prenantes par rapport à la protection des informations confidentielles (Malhotra et al., 2017). Autrement dit, elles pourraient subir des dommages réputationnels et une perte financière subséquente.

La réaction du public envers une entreprise après un vol de données

L'étude de la réaction du public à la suite d'une brèche d'informations confidentielles se caractérise par deux principaux flux méthodologiques. Le premier utilise le cours des actions comme proxy pour mesurer la réaction du public après l'annonce d'une fuite de renseignements personnels (Rosati et al., 2019). Les chercheurs examinent s'il y a une diminution statistiquement significative du cours des actions dans les jours qui suivent une brèche de données (Garg, 2003). Pour s'assurer que la brèche de données soit bel et bien responsable de la baisse en question, les chercheurs contrôlent pour les autres événements qui peuvent avoir un impact sur le cours des actions durant cette période (comme la démission du président-directeur général d'une entreprise)

(Garg, 2003 ; Rosati et al., 2019). La seconde branche d'études, toujours en émergence, emploie l'analyse du sentiment sur les médias sociaux pour quantifier la faute attribuée aux entreprises après une fuite de renseignements personnels. Les médias sociaux, regroupant maintenant 2,95 milliards d'usagers (Clement, 2020), permettent aux internautes d'échanger librement leurs opinions sur une crise donnée avec leurs réseaux sociaux virtuels, un phénomène qui s'appelle le bouche-à-oreille électronique (Austin et Jin, 2012). Une étude de cas sur la brèche au sein d'Equifax en 2017 illustre comment le public s'est divisé en plusieurs communautés pour discuter de l'incident et exprimer leur désagrément sous une même identité numérique (Novak et Vilceanu, 2019). Le bouche-à-oreille électronique prédisant les intentions d'achats des clients (Ismagilova et al., 2019 ; Verhagen et al., 2013), des chercheurs ont commencé à exploiter cette nouvelle source d'informations pour jauger la réaction du public à la suite d'une brèche de données. L'analyse du sentiment collige le langage employé par les utilisateurs sur les médias sociaux à l'aide de techniques algorithmiques, à partir duquel sont examinés les mots, les émoticônes et la structure des phrases (Beigi et al., 2016). Un score indique ensuite si le message est positif, neutre, ou négatif. D'autres chercheurs le combinent avec des techniques de fouille de texte (*text mining*) pour identifier les thèmes de discussion des messages (Syed et Dhillon, 2015).

Un nombre d'approches théoriques est utilisé en conjonction avec ces deux flux méthodologiques pour expliquer les dommages réputationnels après une brèche d'informations. Ainsi, les auteurs qui utilisent le cours des actions s'inspirent typiquement du *Efficient Markets Hypothesis*, c'est-à-dire l'hypothèse que les investisseurs absorbent de façon systématique l'information publique sur le marché et qu'ils ajustent leurs comportements financiers en conséquence, ce qui augmente ou diminue ultimement le cours des actions d'une entreprise (Garg, 2003). Dans le contexte des vols de données, il devrait y avoir un impact préjudiciable sur le rendement boursier de l'organisation victime lorsque les investisseurs pensent que la réaction du public subséquente provoquera une perte financière chez celle-ci (une diminution dans l'intention d'achat, par exemple) (Cavusoglu et al., 2004). Malhotra et Malhotra (2011) ont sinon adopté une perspective centrée sur la « rupture des services » (*service failure*). Selon l'approche, les clients pensent signer un contrat social avec l'entreprise lorsqu'ils donnent volontairement leurs informations confidentielles. Plus spécifiquement, en échange de leurs données confidentielles, les particuliers reçoivent un service personnalisé et convivial. Les données ne sont cependant que

destinées pour l'entreprise et une brèche de données brime donc le contrat social fixé à l'origine (Malhotra et Malhotra, 2011). Une réaction négative des parties prenantes devrait s'ensuivre en conséquence. D'autre part, Syed (2019), dans son analyse des sentiments du public après le vol de données chez Home Depot en 2014, utilise le *Situational Crisis Communication Theory*, une théorie éminente en relations publiques originalement formulée par Coombs (2007). Sommairement, la théorie postule que les individus responsabilisent une organisation pour une crise selon la perception du niveau de contrôle exercé par l'organisation sur les causes. Si le public perçoit qu'un vol de données aurait été facilement évité en présence d'une saine culture de cybersécurité, il devrait tenir l'entreprise hautement responsable de l'événement (Syed, 2019).

Peu importe l'approche méthodologique employée, l'ensemble des écrits révèle que le public réagit mal envers une entreprise touchée par un incident de cybersécurité (Abhishta et al., 2017 ; Cavusoglu et al., 2004 ; Garg et al., 2003). Plus précisément, les parties prenantes expriment des sentiments négatifs, spécialement la colère, lorsqu'ils apprennent d'une brèche d'informations confidentielles (Syed et al., 2019 ; Valecha et al., 2017). D'ailleurs, ce type d'incident suscite davantage de réactions que les autres incidents de cybersécurité touchant exclusivement la composante « intégrité » et « disponibilité » de la cybersécurité parce que contrairement aux autres dimensions, celle de la « confidentialité » est perdue à jamais lorsqu'elle est compromise (Andoh-Baidoo et al., 2010). De plus, Berezina et ses collègues (2012) montrent que cette réaction négative implique tous les clients, que ces derniers soient personnellement touchés ou non par la fuite. Les auteurs ajoutent que la publicité négative engendrée par l'incident réduit les chances qu'une personne continue de fréquenter la firme et augmente la probabilité qu'un client ne recommande pas le service à ses pairs. Cette baisse de compétitivité chez l'entreprise touchée par une brèche d'informations signifie en contrepartie de nouvelles opportunités pour les concurrents du même secteur à accroître leur pouvoir du marché (Jeong et al., 2019). La durée des répercussions économiques qui découlent de la réaction négative du public fait cependant l'objet de débats, avec certains auteurs disant que les dégâts réputationnels qui découlent d'une brèche d'informations perdurent (Cavusoglu, 2004 ; Morse et al., 2011 ; Nieuwesteeg et Faure, 2018), pendant que d'autres affirment le contraire (Acquisti et al., 2006 ; Avery, 2021 ; Ko et Dorantes, 2006). D'une part, il est possible que les particuliers oublient l'incident au fil de l'année et reprennent leurs activités avec la firme comme avant (Ko et Dorantes, 2006). D'autre part, il se peut que les

pratiques de cyber-résilience (un concept qui sera défini ultérieurement) des entreprises jouent un rôle important dans la pérennité des dommages réputationnels après une brèche de données (Avery, 2021 ; Ko et Dorantes, 2006). Cela dit, plusieurs autres facteurs circonstanciels jouent un rôle dans la gravité de la réaction du public à la suite d'une fuite de renseignements.

La taille de l'entreprise

L'impact de la taille de la firme sur la réaction du public après un vol de renseignements personnels apporte des résultats mitigés. Certains chercheurs concluent que le public réagit mal lorsqu'une petite ou moyenne entreprise (PME) est touchée (Cavusoglu et al., 2004 ; Gatzlaff et McCullough, 2010), d'une part parce que les informations compromises ne constitueraient qu'une petite portion des ressources chez une grande entreprise alors qu'elles pourraient représenter l'infrastructure entière d'une PME, et d'autre part parce qu'une grande firme aurait les ressources pour minimiser les dommages causés par la brèche. En revanche, Malhotra et Malhotra (2011) montrent que le public scrute davantage les grandes entreprises, car même si elles ont les moyens pour maîtriser et surmonter l'incident, il est possible que les particuliers s'attendent à ce que les grandes entreprises aient justement plus de ressources que les PME pour prévenir totalement les fuites d'informations. Par ailleurs, une plus grande clientèle pourrait signifier un niveau de propagation plus élevé de bouche-à-oreille au sein des réseaux sociaux. Les résultats de Rosati et *al*. (2019) montrent qu'avec une large clientèle, les grandes entreprises ont de la difficulté à garder sous contrôle le flux d'information médiatique traversant le public. De même, la réaction négative envers les grandes firmes s'exacerbe au fur et à mesure que s'accroît le nombre de clients affectés (Malhotra et Malhotra, 2011). Les mégabrèches de données impliquant des millions de clients risquent dans ce cas d'attirer l'attention des journalistes et d'augmenter les chances d'être assujetties à des recours collectifs, nuisant par la suite à l'opinion générale négative du public envers la grande entreprise en question.

La sévérité du vol de données

La réaction du public est plus sévère lorsque les informations compromises sont de nature financière que si le vol n'implique que des données non financières (Garg et al., 2003 ; Kamiya et al., 2020 ; Malhotra et Malhotra, 2011), au point où une entreprise touchée devient plus susceptible aux poursuites judiciaires (Romanosky et al., 2014). La compromission d'informations financières

entraîne des risques de préjudice plus graves pour les parties prenantes, et il leur serait donc plus facile de légalement réclamer un dédommagement (Romanosky et al., 2014). Le secteur financier se voit d'ailleurs puni plus pour sa victimisation que les autres secteurs, car il stocke justement une grande quantité de données financières et les attentes à l'égard de ses pratiques de cybersécurité s'élèvent en conséquence (Gatzlaff et McCullough, 2010 ; Morse et al., 2011 ; Tweneboah-Kodua et al., 2018 ; Tweneboah-Kodua et al., 2020). Les recherches montrent aussi que la réaction négative à l'égard des fuites de renseignements confidentiels s'aggrave avec le nombre de victimes (Malhotra et Malhotra, 2011). Miller et Angelis (2018) ajoutent que les parties prenantes seront moins disposées à critiquer une entreprise lorsque la brèche est décrite comme ayant affecté un nombre limité de victimes que lorsque l'événement aurait touché des milliers d'individus.

La provenance de l'attaque

Andoh-Baidoo et *al*. (2010) concluent que la réaction du public s'empire lorsque le vol est provoqué par une source externe plutôt qu'interne. Confente et ses collègues (2019) montrent pour leur part que les fuites provoquées par une menace interne malveillante engendrent une réaction négative similaire aux cas impliquant des acteurs externes, à l'exception du fait que les dirigeants sont critiqués pour leur incompétence à contrôler leurs employés. À partir des conclusions de cette étude, il est possible que la faute soit légèrement atténuée lorsque le vol est causé par un acteur externe que lorsqu'il est commis par un acteur interne parce que les coupables dans ce cas se trouvent hors de la portée des politiques de conformité des organisations.

La méthode d'attaque

Les recherches sur la réaction du public à la suite d'un vol de données montrent que les incidents dits *low-tech*, c'est-à-dire les incidents causés par des méthodes comme l'ingénierie sociale et le vol de matériel informatique, exacerbent l'opinion publique négative parce que selon les parties prenantes, ces cas seraient parfaitement évitables dans une organisation qui inspire une saine culture de cybersécurité dans le milieu de travail (Morse et al., 2011). En revanche, les vols de données dits *high-tech*, autrement dit les incidents causés par le piratage informatique, seraient considérés par le public comme étant hors du contrôle immédiat de l'entreprise victime et la réaction négative décroît en conséquence.

La cyber-résilience

Les déterminants de la réaction du public à la suite d'un vol de données qui ont été traitées jusqu'à maintenant relèvent de circonstances se trouvant hors de la portée des entreprises après les faits. En revanche, Knight et Nurse (2020) argumentent que la gestion de cette réaction négative décide ultimement si les dommages réputationnels en question se transforment en menace existentielle pour une firme donnée. Selon certaines sources, les brèches de données peuvent avoir des effets à long terme et ultimement causer la fermeture des entreprises, spécialement les PME (Dhillon, 2015 ; Nieuwesteeg et Faure, 2018). Bien qu'il existe peu de chiffres à ce sujet, le National Cyber Security Alliance (NCSA, 2019) rapporte que parmi les PME ayant subi une brèche de données, le quart a déclaré faillite et 10 % ont fini par fermer définitivement les portes. Les PME occupant la quasi-totalité du marché canadien (Gouvernement du Canada, 2019), il importe de mieux comprendre la cyber-résilience des organisations face à la réaction du public après un vol de renseignements.

Les origines et principes de la cyber-résilience

Le mot « résilience » se tire du verbe latin *resilientia*, qui veut dire « de rebondir » (OED Online, 2020). Dupont (2019) note que le concept fait ses débuts dans la science des matériaux pour désigner la capacité d'une matière à soit maintenir ou revenir à sa forme/position originale après avoir été pliée, étirée ou compressée (OED Online, 2020). Cela dit, l'écologie et la psychologie sont les disciplines responsables de l'explosion du concept dans le monde scientifique (Dupont, 2019). D'une part, les travaux précurseurs de l'écologiste Holling (1973) par rapport à la résilience ont invité les chercheurs à examiner davantage de quelles façons la faune et la flore sont capables de maintenir leurs interactions avec leur écosystème, et ce, malgré les fluctuations imprévisibles de l'environnement. De même, les tragédies mondiales du 20^{e} siècle (comme la Grande Dépression ou la Seconde Guerre mondiale) ont poussé les chercheurs en psychologie à tenter de mieux comprendre les facteurs individuels limitant les séquelles causées par l'adversité, ainsi que d'explorer les éléments favorisant le rétablissement des individus après une épreuve psychologique (Masten, 2018). La résilience décrit dans ce cas la capacité d'une personne à maintenir une croissance individuelle prosociale malgré les événements de vie négatifs ; à maintenir ses aptitudes durant les situations de stress ; et à se remettre des traumatismes psychologiques (Werner, 1995). Le concept de la résilience s'est depuis ce temps frayé un chemin

dans plusieurs domaines dont l'étude des désastres, l'ingénierie mécanique, l'étude des organisations et plus récemment la cybersécurité (Bhamra et al., 2011 ; Dupont, 2019).

Le concept de la résilience est devenu de plus en plus attrayant pour les professionnels de la cybersécurité alors que ces derniers sont maintenant confrontés par l'impossibilité de colmater toutes les failles de sécurité avant leur exploitation par des acteurs malveillants (Dupont, 2019). Le bilan périodique des vulnérabilités logiques sur la liste Common Vulnerabilities and Exposures (CVE, 2021) montre bien comment les entreprises sont submergées par les dangers du cyberespace, et ceci n'inclut pas les vulnérabilités méconnues de tous à l'exception des attaquants (les *zero-days*), ni le soi-disant maillon faible de la cybersécurité, c'est-à-dire le facteur humain (Libicki, Ablon et Webb, 2015). Par ailleurs, les entreprises collaborent de plus en plus avec des parties tierces, formant une chaîne d'approvisionnement complexe dans laquelle sont échangées régulièrement des données, mais qui augmente en contrepartie les points d'accès potentiels pour un contrevenant motivé (Ghadge et al., 2019).

L'avènement de la notion de cyber-résilience reconnaît la futilité derrière la prévention totale des incidents de cybersécurité et préconise conséquemment l'implantation de mesures additionnelles qui aideraient les entreprises à minimiser et à surmonter les divers dommages pouvant découler d'une cyberperturbation (Dupont, 2019). La cyber-résilience sous-entend d'ailleurs que les dégâts qui découlent d'un incident de cybersécurité se font ressentir au-delà de l'infrastructure TI de l'entreprise en touchant également le bon fonctionnement de cette dernière. Le concept s'intéresse donc au maintien continu des activités entrepreneuriales plutôt qu'à la garantie de l'intégrité, la disponibilité et la confidentialité de l'information exclusivement (Bryson, 2018). Par exemple, la redondance des services, c'est-à-dire avoir multiples systèmes qui effectuent la même fonction (NIST, 2015), est une pratique populaire de cyber-résilience, car elle empêche les cyberincidents touchant la composante « disponibilité » de la triade CID d'avoir des répercussions économiques pour une organisation, spécialement dans les cas où un système avec des ressources critiques tombe en panne (Agrafiotis et al., 2018 ; Chapple et Seidl, 2021). De même, les recherches montrent que la violation de la dimension « confidentialité » de la triade CID implique une grave atteinte à la réputation des commerces concernés (Andoh-Baidoo et al., 2010). Se préparer à minimiser et à surmonter la réaction négative du public après une brèche de données

empêcherait celle-ci de se dégénérer en menace existentielle pour les entreprises victimes (Knight et Nurse, 2020). Ainsi, Ponemon (2019) recommande d'employer des stratégies de fidélisation des clients après avoir montré dans un échantillon de 507 entreprises que celles ayant perdu moins de 1 % de leur clientèle après une brèche d'information ont connu une perte moyenne totalisant 2,8 millions $, comparativement à 5,7 millions $ pour les commerces ayant perdu plus de 4 % de leurs clients. Ce constat pourrait d'ailleurs expliquer pourquoi les clients pensent que le service à la clientèle impacte de façon plus importante la réputation d'une entreprise donnée qu'une brèche de données en soi (Ponemon, 2014).

Cela dit, la cyber-résilience ne met pas de côté la prévention et l'absorption des cybermenaces, celles-ci réduisant déjà le nombre d'attaques que l'organisation pourrait devoir surmonter (Bryson, 2018 ; Cichonski et al., 2012). Il s'agit plutôt d'une étape évolutive de la cybersécurité classique où régnait que la prévention des cyberperturbations (Bryson, 2018). Ainsi, plusieurs standards et modèles éminents de cybersécurité intègrent maintenant un semblant de cyber-résilience dans leurs recommandations pour aider les entreprises à améliorer leurs capacités de prévention et de réponse (Dupont, 2019). Par exemple, le National Institute for Standards and Technology (NIST) a conçu l'un des cadres normatifs les plus populaires du marché et plusieurs grandes firmes de cybersécurité comme Accenture (2018) et Symantec (2014) l'ont déjà emprunté pour vendre l'idée de la cyber-résilience au secteur privé. Pareillement, le renommé International Organization for Standardization (ISO) fournit un autre cadre standardisé pour les entreprises (Disterer, 2013).

Rebondir des dégâts réputationnels causés par un vol de données

Afin de protéger sa réputation, tout commerce doit d'abord s'assurer de mettre en place des contrôles de base pour empêcher les vols de données (Knight et Nurse, 2020). Les écrits montrent que les usagers qui critiquent le laxisme dans les politiques de prévention de la cybercriminalité auront davantage tendance à responsabiliser les organisations pour un vol de données et à propager du bouche-à-oreille électronique négatif à leur égard (Knight et Nurse, 2020 ; Syed, 2019 ; Syed et Dhillon, 2015). Par exemple, l'analyse des *tweets* à propos du vol de données chez Home Depot révèle un sentiment général de colère envers la compagnie de vente au détail parce qu'elle aurait négligé de prévenir adéquatement la cybercriminalité :

> “It is past time to consider switching to pin and chip technology” ; “By October 2015 all cards are required to use pin & chip. You were all just too cheap to update to this technology until the last minute.” ; “The reason for all the hacking lately is the mad rush is on to get all the data possible before October next year. With pin and chip, this ends.” (Syed, 2019, p. 266).

De même, Romanosky et *al*. (2014) notent que les vols de données causés par une gestion imprudente des renseignements confidentiels (comme jeter au recyclage les documents en question sans les déchiqueter) augmentent les chances de poursuites judiciaires contre une entreprise. En contrepartie, Ponemon (2017) affirme qu’une gamme de procédés et de technologies complète de cybersécurité aide les entreprises à atténuer et surmonter la réaction négative du public après une brèche de données.

Les lois canadiennes n’indiquent pas explicitement quelles sont les mesures pour lesquelles l’implantation est légalement obligatoire. Ainsi, le CPVPC (2019) signale simplement que les entreprises doivent tenir compte des facteurs suivants lors de la formulation de leurs politiques de sécurité : « la nature délicate des renseignements et le risque de préjudice pour la personne ; la quantité de renseignements ; l’étendue de leur communication ; le format des renseignements ; le type de stockage ; les types et les niveaux de risques auxquels votre organisation est confrontée ».

Il devient alors pertinent de faire la liste des systèmes et actifs d’information en possession et d’identifier lesquels contiennent des données confidentielles sur les parties prenantes et pour lesquelles une compromission serait préjudiciable (Gouvernement du Canada, 2021 ; NCSC, 2020). Les informations personnelles en question pourront ensuite être chiffrées pour empêcher leur mésusage en cas de fuite (Cyber Security Coalition, s.d.). De même, l’identification des menaces possibles auxquelles feraient face ces systèmes et ces actifs permettrait à l’entreprise de déployer ses ressources préventives de manière stratégique (Cyber Security Coalition, s.d. ; NIST, 2018). Selon le rapport annuel de Verizon (2021) sur les brèches de renseignements au sein des organisations, la compromission des identités des acteurs internes explique principalement l’accès non autorisé aux informations confidentielles stockées dans les systèmes et actifs organisationnels.

La compromission des identités s'explique quant à elle particulièrement par l'hameçonnage (Verizon, 2021). Conséquemment, une entreprise pourrait focaliser davantage son attention sur la prévention de l'hameçonnage afin d'empêcher la somme de la compromission des identités et des vols d'informations plus généralement. Les recherches dans ce cas portent spécialement sur la sensibilisation du personnel par l'entremise de tests d'hameçonnage, de jeux éducatifs ou par des formations sur le repérage des courriels d'hameçonnage (Arachchilage et al., 2016 ; Carella et al., 2017 ; Proofpoint, 2020 ; Sheng et al., 2007 ; Wen et al., 2019). D'autre part, les techniques d'apprentissage automatique permettent de détecter et d'arrêter les tentatives d'hameçonnage avant même qu'elles atteignent la boîte de réception d'un employé (Aleroud et Zhou, 2017 ; Alsharnouby et al., 2015). L'implantation de l'authentification à facteurs multiples serait sinon considérée comme la solution d'or pour stopper non seulement l'hameçonnage, mais la compromission des identités en général, car même si une victime divulgue ses informations, l'attaquant percute une seconde couche de sécurité (Maynes, 2019). Les pirates informatiques admettent ne pas s'en prendre aux comptes protégés par l'authentification à facteurs multiples en raison des efforts supplémentaires requis pour la compromission (Mirian et al., 2019). En somme, l'entreprise devrait faire le diagnostic de son écosystème numérique et déterminer quelles options lui sont disponibles pour contrecarrer les vols de données. Par l'entremise d'une certification indépendante octroyée par des organismes de normalisation comme l'ISO, l'entreprise serait en mesure d'argumenter à ses clients qu'elle a fait preuve de diligence raisonnable en matière de prévention des brèches d'informations et de mésusage des données (Cole, 2016). Ceci aura pour effet de réduire la réaction négative subséquente du public (Gwebu et al., 2018 ; Knight et Nurse, 2020). Les résultats de la certification, résumés de manière visuelle, communiquent clairement aux clients le niveau de sécurité de l'entreprise sans les submerger avec des détails de type technique (Matheu et al., 2020).

Se doter d'une bonne capacité de détection permet sinon à l'entreprise de rapidement mobiliser ses mesures de réponse pour limiter la sévérité de l'incident de cybersécurité. Ceci pourrait encore une fois impliquer de sensibiliser le personnel à plusieurs indicateurs possibles d'une brèche, par exemple : (1) les ordinateurs fonctionnent plus lentement qu'à l'habitude ; (2) des utilisateurs sont verrouillés de leurs comptes ; (3) des utilisateurs ne peuvent plus accéder à leurs documents ; (4) des courriels étranges proviennent du domaine de l'organisation (NCSC,

2020). Il existe d'autres solutions de nature technologique, telles que les systèmes de détection d'intrusion et la gestion des événements et informations de sécurité, avec plusieurs auteurs recommandant les alternatives gratuites/source ouverte pour les PME, si ce n'est que pour des raisons strictement économiques (Cichonski et al., 2012 ; Detken et al., 2015 ; Kent et al., 2016). Sinon, la sous-traitance d'une équipe de réponse aux incidents peut dispenser les coûts d'implantation de ces technologies et réduire d'autres coûts relatifs à la formation du personnel pour l'utilisation des outils en question (Carìas et al., 2018). Cette équipe peut aussi s'occuper du confinement de l'incident et de l'éradication des traces de compromission (Morreale, 2008 ; NCSC, 2020).

Si le vol de données est plutôt détecté par une source externe, ceci aura pour effet d'aggraver la réaction négative du public, comme l'exemplifient les *tweets* suivants en lien avec la brèche chez Home Depot : « "The breach first happened in April. Notifying customers quickly?" ; "The notification only came about after an outside security expert blew the whistle." » (Syed, 2019, p.266). Somme toute, une firme doit se munir de capacités de détection adéquates pour rapidement repérer les intrusions et répondre à celles-ci de façon immédiate (Beldad et al., 2018).

L'entreprise peut ensuite s'inspirer des enseignements des étapes de confinement et d'éradication pour communiquer de façon transparente aux parties prenantes les circonstances de la brèche (CIO Strategy Council, 2021). Des chercheurs constatent que fournir des mesures accommodantes, comme dans le cas de Sony PlayStation Network où les clients ont eu accès à des jeux gratuits, des privilèges normalement réservés aux membres et la surveillance du dossier de crédit, réduit la gravité de la réaction négative et les chances d'être assujetti aux poursuites judiciaires (Goode et al., 2017 ; Romanosky et al., 2014). Choi et *al*. (2016) argumentent pour leur part que les mesures accommodantes ne sont pas absolument nécessaires et que le public désire avant tout recevoir une déclaration qui est immédiate, qui exprime du regret, et qui est transparente par rapport aux circonstances de la brèche de même que sur les mesures mises en place pour mitiger les risques de mésusage des informations volées (Gatzlaff et McCullough, 2010 ; Gwebu et al., 2018 ; Jenkins et al., 2014 ; Muzatko et Bansal, 2018). L'avis doit aussi informer les particuliers sur les façons de se protéger des préjudices possibles et émettre les coordonnées de

l'organisation pour les personnes ayant des questions sur l'incident (Choi et al., 2016 ; Cyber Security Coalition, s.d. ; Jenkins et al., 2014). Même si la déclaration publique de l'incident ne s'avère pas obligatoire dans certains cas, l'organisation qui ne souhaite pas lancer d'avis doit juger si les données risquent d'apparaître sur les marchés illicites ou s'il y a risque de lanceur d'alerte (Knight et Nurse, 2020). Quoi qu'il en soit, une déclaration publique donne impression que l'entreprise prend au sérieux la sécurité de ses clients, réduisant conséquemment la sévérité de la réaction du public (Knight et Nurse, 2020 ; Syed, 2019). L'annonce devrait sinon se faire via toutes les chaînes de communication disponibles (courriel, courrier, téléphone, médias sociaux, médias traditionnels) afin de rejoindre le plus de personnes possible (CPVPC, 2018 ; Knight et Nurse, 2020). Un plan de communication dynamique permet ultimement de contrôler le flux d'information par rapport à la brèche (Rosati et al., 2019 ; West, 2016). Bref, la communication de crise, autrement dit le recueil, le traitement et la distribution d'informations nécessaires pour rectifier une situation de crise, est de mise dans le contexte des chocs réputationnels après une brèche de renseignements (Coombs, 2010).

Selon Syed (2019), une entreprise qui omet de mobiliser ses mesures de réponse laisse paraître qu'elle se soucie peu des données de ses parties prenantes et qu'elle met indûment ces dernières en danger, donnant alors l'impression qu'elle est responsable pour le vol de données faute d'une culture de cybersécurité conforme en son sein. De même, Novak et Vilceanu (2019) montrent comment le manque de communication de la part d'Equifax durant sa brèche en 2017 a provoqué une grave réaction négative à son égard. La firme Yahoo a subi quant à elle de grandes pertes dans sa valeur de marque après avoir attendu deux ans pour déclarer une fuite découverte en 2014 (Wang et Park, 2017). Les parties prenantes croiront aussi que l'entreprise sera incapable de surmonter cette crise si leurs démarches médiatiques laissent à désirer (Kim et al., 2019).

Dans les deux semaines qui suivent l'incident, effectuer une séance de « leçons apprises » permet d'ajuster les mesures de prévention, de détection et de réponse et de colmater ainsi les lacunes dans les procédés et technologies de sécurité de l'entreprise (CIO Strategy Council, 2021), faute de quoi elle subira de plus grands chocs réputationnels si une cyberattaque future exploite une même faille (Knight et Nurse, 2020 ; Schatz et Bashroush, 2016).

En somme, une entreprise peut jouer un rôle actif dans la gestion de ses ressources réputationnelles à la suite d'un vol d'informations en adoptant des pratiques qui favorisent sa cyber-résilience. Le constat fait écho à ce que Dupont (2019) appelle la dimension « dynamique » de la cyber-résilience : les chocs réputationnels dans ce cas sont le fruit non seulement de l'incident en soi, mais aussi des décisions prises par la firme en vue de prévenir, contrôler et minimiser les dommages.

Modèle théorique

Les écrits en lien avec la réaction du public à la suite d'un vol de données illustrent l'ambiguïté du statut de victime des entreprises ayant été prises d'assaut par des acteurs malveillants. Ainsi, les firmes victimes d'un vol d'informations en leur sein sont responsabilisées dans une certaine mesure par le public pour avoir manqué de prévenir l'incident, et encore plus si elles n'ont su mobiliser leurs solutions de sécurité et de communication de crise (Choi et al., 2016 ; Gwebu et al., 2018 ; Malhotra et al., 2017 ; Muzatko et Bansal, 2018 ; Novak et Vilceanu, 2019 ; Ponemon, 2017 ; Romanosky et al., 2014 ; Rosati et al., 2019 ; Syed, 2019 ; Syed et Dhillon, 2015). Toutefois, leur statut de victime est d'autant plus flou lorsque sont considérées les obligations formelles des entreprises par rapport à la protection des données. Les lois canadiennes en question peuvent effectivement transformer une firme en ce que Schneider (2014) appellerait une « victime-contrevenante » si celle-ci manque de respecter les exigences en lien avec la prévention et l'annonce des brèches de renseignements. Par exemple, la LPRPDE oblige les entreprises canadiennes concernées de mettre en place des politiques et des pratiques de sécurité adéquates « en fonction du degré de sensibilité des renseignements personnels recueillis, de la quantité, de la répartition et du format des renseignements personnels ainsi que des méthodes de conservation » (CPVPC, 2020, p. 54). La loi encourage sinon le public à soumettre une plainte auprès du CPVPC s'il est jugé que les firmes auraient omis de combler lesdites exigences de sécurité.

Dans l'éventualité où l'atteinte aux informations confidentielles survient malgré la mise en place des mesures de sécurité, la LPRPDE oblige son annonce immédiate si elle risque d'apporter des préjudices considérables aux parties prenantes, qu'elles soient corporelles, réputationnelles ou économiques (CPVPC, 2018). L'évaluation de ces risques est laissée en grande partie à la discrétion de l'organisation, la LPRPDE n'indiquant que vaguement qu'ils se déterminent à partir

du degré de confidentialité des données en cause et de la probabilité qu'elles soient utilisées frauduleusement (CPVPC, 2018). Le CPVPC (2018) prescrit d'inclure dans l'avis : une description globale de la fuite ; une approximation de la date ou la période où il y a eu l'atteinte de sécurité ; la nature des renseignements personnels touchés (si elle est connue) ; les mesures que l'organisation a prises afin d'empêcher le mésusage des données compromises ; les mesures que peuvent prendre les parties prenantes afin de réduire le risque de préjudice découlant de la fuite ; et aussi les coordonnées de l'organisation pour obtenir plus d'informations.

Les organisations qui manquent d'aviser leurs parties prenantes sont passibles d'une amende maximale de 10 000 $ par procédure sommaire, ou 100 000 $ par mise en accusation (CPVPC, 2020). Ainsi, lors de l'année durant laquelle les déclarations sont devenues obligatoires au Canada, le CPVPC (2019) a remarqué une forte multiplication des rapports de brèches de données comparée à l'année précédente. Dans la même veine, le projet de loi 64 au Québec prévoit des sanctions de 15 000 $ à 25 millions $, selon la gravité de l'infraction et des répercussions sur le public (LeBel, 2020). Encore une fois, la ministre de la Justice et ministre responsable de l'Accès à l'information explique que le projet de loi a pour but de « […] responsabiliser les organisations qui utilisent nos renseignements » (Gagnon, 2020).

Tout bien considéré, le statut de victime n'est pas simplement donné à une entreprise ayant subi un vol d'informations, car celle-ci a l'obligation sociale d'agir en tant que gardienne des renseignements personnels de ses parties prenantes (CPVPC, 2018 ; CPVPC, 2020 ; Malhotra et al., 2017). En revanche, une posture de cyber-résilience pourrait permettre la revendication du statut de victime en question (Choi et al., 2016 ; Gwebu et al., 2018 ; Malhotra et al., 2017 ; Muzatko et Bansal, 2018 ; Novak et Vilceanu, 2019 ; Ponemon, 2017 ; Romanosky et al., 2014 ; Rosati et al., 2019 ; Syed, 2019 ; Syed et Dhillon, 2015). En somme, cette perception que la victime partage une partie de la responsabilité pour sa victimisation fait curieusement écho au *Victim Precipitation Theory*, une perspective pionnière de la victimologie, mais controversée pour ses implications de faute sur la victime (Wemmers, 2017).

Le Victim Precipitation Theory, une histoire controversée en victimologie

La notion que la victime pourrait détenir un certain niveau de responsabilité pour le crime qu'elle a subi est caractéristique du premier courant de pensée de la victimologie, celui qui s'intéresse à « l'apport de la victime à la genèse du crime », c'est-à-dire le *Victim Precipitation Theory* (Wemmers, 2017, p. 31). Les typologies pionnières de la victime classifient ainsi cette dernière selon son niveau de responsabilité pour sa victimisation. Par exemple, le modèle de l'éminent victimologue Mendelsohn s'étend de la victime parfaitement innocente (un enfant, une personne inconsciente, etc.) jusqu'à la victime parfaitement coupable (comme un criminel tué dans un cas de légitime défense) (Lasky, 2019). Wolfgang (1957), le premier chercheur à tester empiriquement le *Victim Precipitation Theory*, indique dans son article que le quart des homicides à Philadelphie ont été précipités par la victime. Par exemple, il signale les cas où l'effet désinhibiteur de l'alcool a amené un individu à amorcer une agression physique lui coûtant ultimement sa vie contre sa cible après que celle-ci s'est défendue.

La popularité croissante de la théorie dans l'étude des homicides, des viols, des voies de fait et des vols qualifiés a toutefois été bouleversée par Amir (1968) lorsque celui-ci a argumenté que les victimes de viol partagent la responsabilité de leur victimisation soit parce qu'elles ont cherché à se retirer d'un acte sexuel qu'elles ont consenti au départ ou parce qu'elles ne se sont pas assez débattues contre leur agresseur (Miethe, 1985). Publié pendant la seconde vague du féminisme, il n'a pas tardé avant que les théoriciens de la criminologie critique se mobilisent contre une telle école de pensée, car elle inviterait la faute injustifiée de la victime et l'invalidation de ses expériences traumatisantes (Cortina et al., 2018). Selon Berger et Searles (1985), l'implication que les victimes de viol ont agi de manière à provoquer leur victimisation pourrait diluer la culpabilité du contrevenant et même favoriser son acquittement dans un procès criminel. D'autre part, la notion de *Victim Precipitation* pourrait représenter un élément constitutif du crime. Une victime qui omet de fermer ses fenêtres n'aurait auparavant pas pu dénoncer un cambrioleur à la police pour introduction par effraction parce que ce dernier n'a pas eu besoin de forcer l'entrée avant de se glisser dans la demeure (Gobert, 1977). En somme, Timmer et Norman (1984) argumentent que le *Victim Precipitation Theory* contribue au maintien du statu quo, car celle-ci laisse présager que c'est à l'individu de prendre les précautions nécessaires pour prévenir le crime (comme se vêtir de

façon moins provocatrice, barrer ses portes, etc.), et ce, au détriment des pistes d'intervention visant les causes structurales du crime (comme la pauvreté, le racisme systémique, etc.).

Les conséquences de la faute de la victime sont bien illustrées dans les recherches de Cross et *al*. (2019) : la fuite de données chez *Ashley Madison*, une plateforme de rencontre extra-conjugale, a provoqué de graves répercussions réputationnelles chez les individus touchés en raison de la nature immorale du site ainsi que de ses abonnés, et en a même mené certains au suicide. Par ailleurs, des victimes de fraude à l'identité dans l'étude de Jansen et Leukfeldt (2018) disent avoir été traitées comme les responsables des transactions frauduleuses et qu'elles ont ressenti le besoin de prouver leur innocence aux banques. D'autre part, les victimes de fraude dans l'étude de Cross et ses collègues (2016) expriment avoir été scrutées par leurs proches et avoir vécu des répercussions affectives négatives en conséquence. Le phénomène de la faute de la victime ayant des effets néfastes sur le bien-être émotionnel des victimes, il n'est pas surprenant de constater que ces dernières craignent de signaler leur victimisation aux autorités et de solliciter de l'aide psychologique (Cross et al., 2016 ; Morrison et al., 2006 ; Sable et al., 2006 ; Schwarz et al., 2017).

Le modèle classique de la victime « idéale »

Alors que le prochain courant de la victimologie dirige son attention vers les besoins des victimes (Wemmers, 2017), certains chercheurs, notamment de la perspective féministe, se sont appropriés les idées fondatrices du champ d'études pour mieux comprendre la réaction sociale envers les victimes d'agression sexuelle et la pérennisation des mythes de l'agression sexuelle (Cowan, 2000 ; Fox et Cook, 2011 Janoff-Bulman et al., 1985 ; Lutz-Zois et al., 2015 ; Marciniak, 1998). En particulier, les écrits sur le *Just World Theory* notent bien comment les victimes d'agression sexuelle sont souvent responsabilisées pour des événements qu'elles n'ont pu objectivement contrôler (Correia et Vala, 2003 ; Strömwall et al., 2013). Le *Just World Theory* se réfère au besoin psychologique du public de penser que le monde est juste (Lerner et Miller, 1978). Lorsqu'un acte injuste survient, comme un viol, la théorie soutient que le public maintient sa croyance en un monde juste en argumentant que, d'une manière ou d'une autre, la victime a précipité sa victimisation (Lodewijkx et al., 2001). Ainsi, les individus avec de fortes croyances en un monde juste ont tendance à être d'accord avec des mythes du viol comme « si une femme

rentre dans la demeure d'un homme après leur première sortie, elle a déjà donné son consentement sexuel » (Hayes et al., 2013 ; Vonderhaar et Carmody, 2015). D'autres chercheurs ont d'ailleurs utilisé la théorie pour expliquer la faute sur la victime dans le contexte d'autres crimes, par exemple les vols qualifiés (van den Bos et Maas, 2009) et les crimes haineux (Dharmapala et al., 2009).

Si la somme des recherches montre que les individus ont tendance à mettre en cause les victimes pour ce qui leur est arrivé, d'autres ajoutent que certaines victimes seront mieux traitées que d'autres par le public. Par exemple, Gilmartin-Zena (1983) a présenté deux vignettes de cas à un échantillon de 150 étudiants universitaires en vue de susciter des jugements envers une victime de viol. D'une part se trouve la victime « idéale » : la femme mariée, habillée de façon conservatrice, qui s'est gravement blessée en se débattant contre un agresseur inconnu. D'autre part figure la victime « non-idéale » : la femme divorcée, habillée de façon provocatrice, qui est restée passive contre un attaquant qu'elle connaît et qui a subi l'événement sans graves blessures physiques. Les participants attribuent effectivement un plus grand niveau de responsabilité à la victime « non-idéale » qu'à la victime « idéale » pour le viol.

L'idée de la victime « idéale » a surtout gagné en popularité depuis la conceptualisation de Christie (1986). Le criminologue affirme qu'être une victime n'est pas un phénomène objectif et que son obtention dépend plutôt de la manière dont les individus perçoivent les circonstances entourant la victimisation. Selon Christie (1986), le public octroie le plein statut de victime à une personne ou un groupe frappés par le crime que lorsque ceux-ci présentent les cinq caractéristiques principales de la victime « idéale » : (1) elle est « fragile » ; (2) elle mènerait un projet « respectable » au moment de sa victimisation ; (3) elle est « irréprochable » ; (4) le contrevenant est « imposant » ; (5) le contrevenant est un « inconnu ».

Pour illustrer son modèle, Christie (1986) utilise l'analogie de la vieille dame (victime « fragile ») qui, après s'être occupée de sa sœur malade (projet « respectable »), retourne chez elle durant la journée (victime « irréprochable »), mais qui devient en chemin l'objet d'un vol qualifié par un étranger (contrevenant « inconnu ») de grande taille (contrevenant « imposant »). Christie (1986) ajoute toutefois une mise en garde dans son modèle conceptuel : la victime doit démontrer suffisamment de « puissance » pour revendiquer politiquement son statut de victime. Selon lui, les

vieilles dames et leur relation de dépendance avec la société suscitent la pitié, et le public serait alors prêt de les donner le statut de victime. Le modèle de Christie (1986) forme une hiérarchie de statut de victime et la position dans laquelle s'y trouve un individu détermine le niveau de responsabilité qui lui est attribué pour sa victimisation (Mason, 2013).

Plusieurs articles en lien avec la réaction sociale de la victimisation ont depuis ce temps référé au concept de la victime « idéale » (Alexius, 2020; Cross et al., 2019; Mason, 2013; van Wijk, 2013; Zaykowski et al., 2014), mais comme le précisent Lewis et *al*. (2019), il existe peu d'études empiriques sur la façon dont les dimensions du modèle se manifestent dans le discours du public. Leur analyse linguistique sur les conceptualisations populaires vis-à-vis aux victimes montre ainsi que l'attribution du statut de victime dépend davantage des caractéristiques de la victime que de celles du contrevenant. Autrement dit, elle concerne plus les dimensions « victime fragile », « projet respectable » ainsi que « victime irréprochable » du modèle de la victime « idéale » plutôt que les aspects « contrevenant inconnu » et « contrevenant imposant ». En même temps, les auteurs n'ont pu trouver de citations se rapportant à la dimension « suffisamment puissante » de la victime « idéale ». Cela dit, l'appui empirique des diverses qualités de la victime « idéale » laisse toujours à désirer.

L'entreprise victime « idéale »

Hopkins (2016) souligne que les définitions classiques de la victimologie comme discipline insistent sur l'étude scientifique de la victimisation des individus. Les études en victimologie sur la faute de la victime qui ont été citées ici jusqu'à présent n'ont bel et bien porté que sur les individus. Cependant, Hopkins (2016) affirme que ceci met nécessairement de côté les expériences des entreprises alors que le crime percute plus fréquemment ces dernières que les particuliers. De nombreux auteurs ont noté qu'il existe très peu de connaissances en lien avec la victimologie des entreprises et que les enquêtes en lien avec ce champ d'études sont rarissimes (Hopkins, 2016 ; Schneider, 2014 ; Stockman et al., 2017). Par exemple, l'Enquête sociale générale (ESG) exclut les crimes commis contre les organisations (Moreau, 2021). Ce n'est qu'en 2017 que l'Enquête canadienne sur la cybersécurité et le cybercrime a été lancée pour mesurer l'incidence de la cybercriminalité sur les entreprises canadiennes (Statistique Canada, 2020).

Selon Hopkins (2016), les entreprises ont tendance à être dépeintes comme étant des contrevenantes plutôt que des victimes ; l'étude de la criminalité en col blanc vient ici vite à l'esprit. Après tout, Sutherland (1940), pionnier de la recherche sur la criminalité en col blanc, souligne bien comment les coûts de l'ensemble des crimes en col blanc excède grandement ceux des crimes conventionnels :

> An officer of a chain grocery store in one year embezzled $600,000, which was six times as much as the annual losses from five hundred burglaries and robberies of the stores in that chain. Public enemies numbered one to six secured $130,000 by burglary and robbery in 1938, while the sum stolen by Krueger is estimated at $250,000,000, or nearly two thousand times as much (Sutherland, 1940, p. 5).

Des auteurs ont plus récemment noté qu'outre les milliards de dollars en pertes économiques, la criminalité en col blanc nuit davantage au bien-être psychologique des victimes, à l'environnement et à la confiance publique envers les institutions politiques ainsi qu'économiques, comparativement aux crimes conventionnels (Billings et al., 2021 ; Cohen, 2013). Cela dit, McGurrin et al. (2013) soulignent par une analyse du contenu des écrits scientifiques que même ce sous-domaine de la criminologie reste peu étudié comparé à la criminalité conventionnelle. Le concept même de la criminalité en col blanc a été le sujet de plusieurs débats entre scientifiques, au point où le White-Collar Crime Center a décidé d'organiser un atelier regroupant les spécialistes sur le sujet dans le simple but d'en arriver à un consensus sur une définition (Reurink, 2016), qui est la suivante : « Illegal or unethical acts that violate fiduciary responsibility or public trust, committed by an individual or organization, usually during the course of legitimate occupational activity, by persons of high or respectable social status for personal or organizational gain » (Helmkamp et al., 1996, p. 351). Sinon, lorsque les firmes sont elles-mêmes les victimes de fraude interne, la loi peut toujours les tenir responsables des agissements d'un employé malveillant, et les poursuites judiciaires ont effectivement tendance à viser l'entièreté de la firme au lieu de la personne ayant commis le crime en question (Fisse et Braithwaite, 1986 ; Schneider, 2014). Le même constat peut être aperçu dans les lois canadiennes sur la protection des données, que la brèche soit de source externe ou interne (CPVPC, 2020 ; von Tigerstrom, 2018).

À la lumière des propositions de Christie (1986), Hopkins (2016) se demande quelle place occupe la notion de la victime « idéale » dans le contexte des crimes contre les entreprises. De manière générale, les crimes commis contre les commerces sembleraient générer peu de sympathie d'une part parce les entreprises sont perçues comme des entités inanimés et dépourvues d'émotions (Australian Institute of Criminology, 2004), mais aussi parce que le public croit qu'elles auraient les ressources pour absorber les coûts liés à la criminalité, contrairement aux victimes individuelles (Johnston et al., 1994). Cette indifférence contribuerait à la difficulté des entreprises à obtenir le statut de victime, créant subséquemment une culture dans laquelle les crimes commis contre les commerces sont tolérés (Australian Institute of Criminology, 2004). Par exemple, les recherches adoptant le cadre des techniques de neutralisation (Sykes et Matza, 1957) montrent comment les délinquants emploient le déni du mal pour se déculpabiliser des crimes contre les firmes (Ingram et Hinduja, 2008 ; Rieb et al., 2017) :

> They [stores] big. Make lotsa money. They don't even miss the little bit I get. (19-year-old male) ; They write it off their taxes. Probably make a profit off it. So, nobody gets hurt. I get what I need and they come out O.K. too. (28-year-old male) ; Them stores make billions. Did you ever hear of Sears going out of business from boosters? (34-year-old female) (Cromwell et Thurman, 2003, p. 543).

Même si Hopkins (2016) doute que les commerces soient capables d'obtenir le même statut de victime que celui de la vieille dame dans l'analogie de Christie (1986), il a conçu un modèle préliminaire de la victime « idéale » adapté pour les entreprises. Il affirme que le concept demeure pertinent même dans le contexte de la victimisation des entreprises parce qu'il implique tout de même une forme de continuum et les recherches futures peuvent donc identifier les facteurs qui assurent une meilleure revendication du statut de victime chez les firmes.

Dans le cadre de son modèle, Hopkins (2016) reprend les cinq qualités de la victime « idéale » telles que décrites par Christie (1986). Ainsi, l'entreprise victime « idéale » est avant tout « fragile » : elle est vulnérable au crime parce qu'elle n'a pas les moyens de s'en protéger, et elle le subit donc de pleine force (Hopkins, 2016). L'auteur se réfère ici aux petites et moyennes entreprises. Leur budget étant restreint, les PME préfèrent investir les ressources qu'elles ont sur

la croissance des affaires au lieu de la sécurité (Heidt et al., 2019 ; Ng et al., 2013). Les PME seraient déresponsabilisées parce qu'en vertu de leur « fragilité » économique, se protéger adéquatement de la criminalité serait hors de leur portée (Hopkins, 2016). Les recherches empiriques par rapport à cette affirmation demeurent cependant peu concluantes dans le contexte des vols de renseignements (Cavusoglu et al., 2004 ; Gatzlaff et McCullough, 2010 ; Malhotra et Malhotra, 2011 ; Rosati et al., 2019).

En deuxième lieu, l'entreprise effectue un projet « respectable ». Hopkins (2016) mentionne qu'une firme victime doit poursuivre un mandat légal et moralement acceptable. Toutefois, il ajoute qu'il est davantage important que le crime suscite une indignation morale en faveur de la victime, et ce, même si la moralité de certains commerces (comme les banques, les casinos et les boîtes de nuit) pourrait être mise en doute. Hopkins (2016) affirme alors que les crimes violents commis contre le personnel d'une entreprise donnée pourraient diriger la réaction du public vers les agresseurs. La recension des écrits a révélé que dans tous les cas, les brèches de sécurité et les vols de données plus spécifiquement suscitent une certaine réaction négative du public à l'égard de l'entreprise victime, spécialement si les incidents exposent les données financières d'un grand nombre de parties prenantes (Garg et al., 2003 ; Gatzlaff et McCullough, 2010 ; Kamiya et al., 2020 ; Malhotra et Malhotra, 2011 ; Miller et Angelis, 2018 ; Morse et al., 2011 ; Romanosky et al., 2014 ; Tweneboah-Kodua et al., 2018 ; Tweneboah-Kodua et al., 2020).

En troisième lieu, l'entreprise est « irréprochable », c'est-à-dire que la firme est épargnée de la responsabilisation parce que le crime est survenu malgré les précautions qu'elle a pu mettre en place pour décourager la criminalité (Hopkins, 2016). Celle qui ne prend aucune mesure pour dissuader la criminalité serait vue comme étant responsable de sa victimisation parce qu'elle aurait présenté des opportunités criminelles alléchantes aux délinquants. La revue de littérature a montré que les organisations qui omettent d'implanter adéquatement des mesures de protection des données vivent une plus grave réaction du public (Syed, 2019 ; Syed et Dhillon, 2015). Dans le contexte des vols de données, cette dimension du modèle de la victime « idéale » inclut aussi d'autres pratiques de cyber-résilience, plus spécifiquement les mesures de réponse activées par les entreprises pour réduire les risques de mésusage des données (Gwebu et al., 2018 ; Jenkins et al., 2014 ; Muzatko et al., 2018 ; Syed, 2019). Pour réitérer, Syed (2019) argumente qu'une entreprise

qui ne mobilise pas ses capacités de réponse risque de transmettre au public une image négative par rapport à sa culture entière de cybersécurité et qu'elle serait, tant bien que mal, vue comme étant responsable du vol en raison de sa négligence perçue en matière de protection des données.

En quatrième lieu, le criminel est un « inconnu ». Selon le modèle de Hopkins (2016), un commerce victime d'une fraude interne ne serait nécessairement pas une victime « idéale » parce que l'organisation en question connaîtrait le contrevenant. En cybersécurité, bien que les efforts de protection de données se concentrent sur les menaces externes, la médiatisation de la menace interne malveillante met en lumière le fait que le danger de compromission des données ne guette pas exclusivement à l'extérieur de leur infrastructure (Kont et al., 2018 ; Saxena et al., 2020 ; Verizon, 2021). Les résultats restent cependant mitigés par rapport à l'impact de la provenance de l'attaque sur le niveau de responsabilisation de l'organisation après un vol de données (Andoh-Baidoo et al., 2010 ; Confente et al., 2019).

En cinquième lieu, le crime nécessite un contrevenant « imposant » : il utilise des méthodes astucieuses pour commettre son crime, ou encore il est lié au crime organisé (Hopkins, 2016). Dans le contexte des vols de données, la réaction du public envers une organisation victime est moins sévère si les cybercriminels ont employé des méthodes techniques pour lancer leur cyberattaque contre l'infrastructure hébergeant les informations personnelles (Morse et al., 2011). Ce constat renvoie à une notion populaire dans les médias et le discours politique, celle du *super-hacker* ou du *super-user*. Le *super-hacker/super-user* est le pirate informatique surdoué qui a à portée de main la capacité de neutraliser la société contemporaine entière (Wall, 2008). Les firmes ne peuvent se préparer adéquatement contre celui-ci, car le mythe soutient qu'il est difficile à trouver, qu'il maîtrise parfaitement les technologies numériques et qu'il sait exploiter les failles dans la loi pour échapper aux poursuites judiciaires (Ohm, 2008). En réalité, les cyberdélinquants tirent surtout avantage du facteur humain de la cybersécurité par l'entremise d'attaques d'ingénierie sociale (Sjouwerman, 2017). Autrement dit, les vols de données sont principalement causés par un employé ayant malencontreusement divulgué ses privilèges d'accès à un acteur malveillant (Verizon, 2021). Toutefois, comme l'indiquent Morse et *al.* (2011), les organisations touchées deviennent dans ce cas des victimes « non-idéales ».

Enfin, l'entreprise est suffisamment « puissante » : une firme, même si elle est « fragile », est capable de politiquement revendiquer son statut de victime (Hopkins, 2016). Selon Hopkins (2016), les partenariats public-privé dévoués à la lutte contre la criminalité ont réussi à conscientiser la population à la victimisation des entreprises. De même, les forces policières ont fait alliance avec le secteur privé pour lutter plus spécifiquement contre la cybercriminalité (Boes et Leukfeldt, 2016). Par exemple, le Groupe national de coordination contre la cybercriminalité (GNC3) est un partenariat public-privé dont le but est : « de réduire la menace, les répercussions et le nombre de victimes de la cybercriminalité au Canada » (Gendarmerie royale du Canada, 2020). L'avènement des partenariats public-privés réorienterait, selon Hopkins (2016), l'attention vers la poursuite des délinquants et rendrait plus saillant le statut de victime de l'entreprise.

Les dimensions prescrites dans le modèle de l'entreprise victime « idéale » illustrent pourquoi certaines firmes seraient davantage responsabilisées que d'autres pour leur victimisation (Hopkins, 2016). Le projet de recherche ci-présent utilise les idées de Hopkins (2016) afin d'étudier le statut de victime d'une entreprise ayant subi un vol de données, et ce, selon sa qualité « irréprochable », c'est-à-dire sa posture de cyber-résilience. Dans le cas de ce projet de recherche, la posture de cyber-résilience en question inclut les mesures de prévention et de réponse prouvées dans la revue de littérature comme ayant un bienfait sur la réputation d'une entreprise après une brèche de données. Ceci inclut la mise en place adéquate de contrôles préventives de sécurité, de chiffrement des données et de mécanismes de communication de crise. Les autres dimensions pertinentes de la victime « idéale » sont contrôlées en conséquence dans le modèle d'analyse.

Problématique

Limite des connaissances actuelles

Les vols de renseignements personnels représentent une réalité incontournable pour les firmes alors que celles-ci accueillent la cueillette, le stockage et l'analyse des données dans leurs plans d'affaires (Dupont, 2019 ; Rosati et al., 2019). Or, malgré l'inévitabilité des incidents actuels de cybersécurité (Dupont, 2019), l'ensemble des particuliers s'attend toujours à ce que les entreprises prennent les mesures adéquates pour prévenir, détecter et répondre à la compromission de leurs données (Bentley et al., 2018). Les commerces qui manquent à cette obligation risquent de subir une réaction désastreuse du public et de vivre subséquemment un bouleversement

économique irréparable (Knight et Nurse, 2020). Cela dit, la littérature scientifique portant sur ces dommages de nature réputationnelle reste peu développée, et ce, malgré le fait qu'ils représentent l'inquiétude principale des chefs d'entreprises après une cyberattaque (Ponemon, 2017 ; The Economist Intelligence Unit, 2016). Ce manque de connaissances pourrait s'expliquer avant tout par une difficulté à obtenir des données fiables sur le sujet. Les perspectives recueillies des firmes et des individus peuvent présenter un portrait biaisé des brèches de données parce qu'il est parfois difficile de jauger avec précision sa nature et ses impacts, ces derniers pouvant s'étaler sur plusieurs années (Coffey, 2019). Par ailleurs, même après la détection d'une cyberattaque préjudiciable, certaines entreprises sont réticentes de remplir leur obligation légale de le déclarer publiquement justement parce qu'elles craignent les répercussions réputationnelles (Holt, 2017 ; Richardson, 2011). En outre, les lois canadiennes sur l'avis obligatoire des brèches d'informations ne précisent pas quel incident serait considéré comme étant préjudiciable et méritant donc un avis public (CPVPC, 2018). Comme le suggèrent Sullivan et Maniff (2016), les entreprises pourraient, intentionnellement ou non, mal évaluer la gravité de la fuite et décider de ne pas l'annoncer. Qui plus est, les audits de sécurité ne sont pas capables de faire la différence entre la dissimulation et l'ignorance d'un commerce à propos d'une intrusion en leur sein (Laube et al., 2016). Outre les implications réputationnelles, les organisations ne s'importunent pas de signaler les cyberattaques aux forces de l'ordre parce qu'elles ne croient pas que la police peut les aider à rectifier les incidents impliquant la cybercriminalité (Richardson, 2011). Il devient spécialement difficile pour la police d'appréhender le coupable si le cybercrime en question a été commis à l'extérieur de leur compétence juridique (Cross, 2020 ; Dupont, 2017 ; Huey et al., 2012). En bref, les données policières sur la problématique des brèches de renseignements sont rarissimes (Richardson, 2011).

Il est important aussi de noter que la cybercriminologie en tant que domaine d'études n'a simplement pas connu d'essor jusqu'à aujourd'hui (Bossler et Berenblum, 2019). Auparavant, les éditeurs des journaux de criminologie ne considéraient pas la cybercriminalité comme étant un « vrai crime » et invitaient les chercheurs à plutôt publier leurs résultats dans les journaux d'informatique et de cybersécurité. S'ajoute le manque d'intérêt pour la victimologie des entreprises, tel que souligné par Hopkins (2016). Les rapports provenant du secteur privé de la cybersécurité comblent dans une certaine mesure le vide intellectuel en lien avec la prévalence et

les impacts de la cybervictimisation sur les entreprises, mais il demeure qu'ils n'ont pas la même rigueur scientifique que les articles scientifiques avec comité de pairs (Holt, 2017).

La majorité des études qui existent sur les impacts réputationnels des brèches de données s'en tiennent quant à elles de prouver l'apparition d'une réaction négative du public à l'égard des entreprises touchées, mais très peu explorent les dimensions qui exacerbent ou minimisent sa gravité. D'autre part, même les articles qui vont jusqu'à discuter des déterminants de la réaction du public n'abordent pas nécessairement le rôle important que jouent les pratiques organisationnelles de cyber-résilience dans la survie des commerces. Par exemple, les recherches sur la taille de l'entreprise (Cavusoglu et al., 2004 ; Gatzlaff et McCullough, 2010 ; Malhotra et Malhotra, 2011 ; Rosati et al., 2019), la provenance de l'attaque (Andoh-Baidoo et al., 2010 ; Confente et al., 2019) ou encore la méthode d'attaque (Morse et al., 2011) sont des caractéristiques que les entreprises ne peuvent contrôler lorsque vient le temps de répondre à un incident de cybersécurité. De même, l'appui empirique lié à la cyber-résilience et à son impact sur la réaction du public après un vol de données demeure fragmenté, et ainsi les articles qui examinent les bienfaits de certaines stratégies de réponse, comme la déclaration immédiate de la brèche (Muzatko et Bansal, 2018) ou les mesures accommodantes (Goode et al., 2017), ne se réfèrent pas au concept plus large de la cyber-résilience.

En raison du manque de connaissances explicatives en lien avec les déterminants des chocs réputationnels après un vol de données, et plus spécifiquement sur les mécanismes promouvant la cyber-résilience, l'utilité sociale du concept en question est mise en doute par certains professionnels de la cybersécurité (Dupont, 2018). Méconnaissant la posture à prendre pour protéger adéquatement leur réputation, les entreprises victimes pourraient aussi être incitées à exploiter le laxisme légal par rapport à la forme de l'avis public et banaliser ou rendre ambigu la gravité de l'incident afin de limiter les dommages réputationnels (Bisogni, 2016 ; Jackson et al., 2019). Ceci a ultimement comme effet de peu habiliter les parties prenantes face à la fraude à l'identité (Zou et al., 2018).

Objectifs de l'étude

À la lumière de cette limite des connaissances actuelles et de ses conséquences possibles, l'objectif principal de ce projet de recherche est d'expliquer l'impact d'une posture de cyber-résilience sur la réaction du public à la suite d'un vol de données chez les entreprises. À partir des réactions identifiées dans la recension des écrits, l'étude divise la réaction en deux volets — les attitudes et les comportements du public (Ablon et al., 2016 ; Choi et al., 2016, Kim et al., 2019 ; Romanosky et al., 2014 ; Syed, 2019 ; Syed et Dhillon, 2015 ; Valecha et al., 2017). Cette démarche permet de comprendre si les attitudes négatives du public impliquent aussi des répercussions tangibles pour l'organisation en faute et comment une posture de cyber-résilience atténue le tout. De là découlent trois objectifs spécifiques.

En premier lieu, il est nécessaire d'examiner l'impact d'une posture de cyber-résilience sur les attitudes du public à l'égard des entreprises après un vol de données. Les attitudes regroupent l'ensemble des évaluations (favorables ou défavorables) qu'une personne fait à l'égard d'une entité (Ajzen et Fishbein, 1978). La revue de littérature a relevé trois principaux indicateurs attitudinaux après un vol de données : le niveau de responsabilité attribué à l'entreprise, les sentiments négatifs ressentis à son égard ; et la croyance qu'elle peut surmonter la crise. Par l'entremise d'une échelle ordinale, les participants de cette étude doivent indiquer leur niveau d'accord ou de désaccord pour chacune de ces attitudes.

Le second objectif spécifique est de jauger l'impact d'une posture de cyber-résilience sur les intentions comportementales du public à l'égard des entreprises après un vol de données. Contrairement aux attitudes, les comportements sont des actions prises par un individu (Ajzen et Fishbein, 1978), dans ce cas par rapport au commerce. Cette étude mesure les intentions de prendre lesdites actions. La recension des écrits a noté un lien entre les vols de données et trois indicateurs comportementaux des particuliers envers la firme victime : le bouche-à-oreille, l'intention d'achat et l'intention de faire des poursuites judiciaires. Comme pour les attitudes, les répondants du sondage ci-présent signalent leur degré d'accord ou de désaccord pour les trois comportements susmentionnés.

Enfin, il est pertinent de déterminer l'association entre les attitudes et les intentions comportementales du public envers les entreprises après un vol de données. Cet objectif spécifique teste l'argumentaire du *privacy paradox* (Barnes, 2006), c'est-à-dire le fait que malgré les fortes convictions qu'ils peuvent avoir par rapport à la protection de leur vie privée, les internautes font peu pour montrer qu'ils se préoccupent réellement de la sécurité de leurs informations. Martin et *al*. (2020) affirment que le phénomène n'existe pas, du moins dans le contexte des brèches de données, car les particuliers, pensant sincèrement que c'est aux entreprises de protéger leurs données, punissent celles qui manquent de protéger l'intégrité de leur vie privée. Il y aurait *privacy paradox* si les clients mettaient la faute sur l'entreprise pour le vol d'informations et entretenaient des sentiments ainsi que des croyances négatives vis-à-vis celle-ci, sans pour autant modifier leurs habitudes de consommation. Cet objectif spécifique cherche également à montrer si les dommages de nature réputationnelle découlant d'un vol de renseignements sont associés à un impact préjudiciable sur la performance économique d'un commerce donné et ont alors des implications pour la cyber-résilience de celui-ci (Knight et Nurse, 2020). Le tableau 1 résume les objectifs du projet de recherche :

Tableau 1 : Objectif principal et objectifs spécifiques du projet de recherche

<table>
<tr><td colspan="2">OBJECTIF PRINCIPAL

Expliquer l’impact d’une posture de cyber-résilience sur la réaction du public à la suite d’un vol de données chez les entreprises</td></tr>
<tr><td>OBJECTIF SPÉCIFIQUE 1
(VOLET ATTITUDINAL)

Expliquer l’impact d’une posture de cyber-résilience sur les ATTITUDES du public à la suite d’un vol de données chez les entreprises</td><td>OBJECTIF SPÉCIFIQUE 2
(VOLET COMPORTEMENTAL)

Expliquer l’impact d’une posture de cyber-résilience sur les INTENTIONS COMPORTEMENTALES du public à la suite d’un vol de données chez les entreprises</td></tr>
<tr><td>ATTITUDES MESURÉES

Niveau de responsabilité attribué à l’entreprise victime
Sentiments négatifs ressentis à l’égard de l’entreprise victime
Croyance que l’entreprise victime peut surmonter la crise</td><td>INTENTIONS COMPORTEMENTALES MESURÉES

Le bouche-à-oreille
L’intention d’achat
L’intention de faire des poursuites judiciaires</td></tr>
<tr><td colspan="2">OBJECTIF SPÉCIFIQUE 3

Déterminer l’association entre les attitudes et les intentions comportementales du public envers les entreprises après un vol de données</td></tr>
</table>

Le modèle de la victime « idéale » adaptée pour les entreprises (Hopkins, 2016) est un cadre théorique pertinent pour explorer la réaction du public à l’égard d’une entreprise ayant subi un vol de données parce que comme le laisse présager la recension des écrits, la gravité des dommages réputationnels impliqués peut dépendre de la mesure dont une firme concernée exhibe les qualités de la victime « idéale ». Dans cette étude, la posture de cyber-résilience d’une entreprise constitue la qualité « irréprochable » de la victime « idéale » (Hopkins, 2016). L’approche expérimentale de ce projet de recherche permet sinon de contrôler les autres dimensions du modèle qui ne relèvent pas nécessairement des solutions organisationnelles de cyber-résilience, mais qui influencent tout de même la réaction du public à la suite d’un vol de données. Les données ayant été recueillies, les analyses statistiques subséquentes permettent de répondre aux objectifs de recherche et de tester la validité des dimensions de la victime « idéale » dans le cas de la victimisation des entreprises.

En plus d'une meilleure compréhension de la cybercriminalité et de ses impacts, la notion plus précise de la cyber-résilience, qui a joui d'une attention principalement conceptuelle (Dupont et al., 2020), gagne un certain fondement empirique. Le concept en retire également une pertinence sociale, parce qu'il serait avantageux pour les chefs d'entreprises de savoir si une posture de cyber-résilience les aiderait réellement à rebondir des dégâts réputationnels tant redoutés après une brèche de sécurité (Ponemon, 2017 ; The Economist Intelligence Unit, 2016). Les particuliers bénéficieraient aussi d'une meilleure protection de leurs données et d'une meilleure réponse au cas où celles-ci soient compromises. D'autre part, ce projet de recherche teste la pertinence de la notion de victime « idéale » pour les firmes et contribue plus généralement à la victimologie des entreprises, un domaine peu développé de la criminologie.

CHAPITRE 2 — MÉTHODOLOGIE

Le projet de recherche ci-présent explore les dommages réputationnels causés par les vols de données. Plus spécifiquement, il évalue l'impact d'une posture de cyber-résilience sur la réaction du public à la suite d'un vol de données chez les entreprises. Pour remplir cet objectif, l'étude privilégie une démarche expérimentale à base de vignettes de cas, dans laquelle sont traitées les différentes dimensions du modèle de la victime « idéale » adapté pour les entreprises (Hopkins, 2016).

La majorité des études qui portent sur la faute de la victime adoptent une approche méthodologique fondée sur les vignettes de cas, où les participants lisent une mise en situation dans laquelle sont manipulées les caractéristiques de la victime et du scénario tel quel (Alexander et Becker, 1978 ; van der Bruggen et Grubb, 2014). Ils répondent ensuite à un sondage, sur lequel ils émettent des jugements à l'égard de la victime mise en lumière dans la vignette de cas en question. La variation systématique des caractéristiques des scénarios permet de mesurer les impacts des diverses combinaisons de variables à l'étude sur les attitudes des individus (Alexander et Becker, 1978). Une étude avec 3 variables dichotomiques quelconques impliquerait ainsi un total de $2^3 = 8$ différentes vignettes. Par exemple, Ayala et *al*. (2018) ont invité des étudiantes universitaires à lire une de huit vignettes de cas décrivant un viol. Les participantes communiquent ensuite dans quelle mesure elles responsabilisent la victime et le contrevenant, et ce, en fonction : (1) du genre de la victime (homme/femme) ; (2) du genre de l'agresseur (homme/femme) ; (3) de la relation entretenue entre la victime et l'agresseur (viol commis par une connaissance/viol commis par un inconnu). Le niveau d'acceptation des mythes du viol des participantes a aussi été mesuré. Par l'entremise de cette méthodologie, les chercheuses expliquent d'abord que la faute sur la victime d'un viol prévaut si le contrevenant est de genre féminin. La faute de la victime se manifeste aussi si le violeur est de genre masculin et que le répondant adhère fortement aux mythes du viol.

Les expériences à base de vignettes de cas permettent au chercheur de fixer ses variables au sein d'un milieu contrôlé, ce qui a pour effet de faciliter l'interprétation des résultats parce que les impacts perçus peuvent être aisément attribués à la démarche expérimentale (Finch, 1987). L'étude de Hainmueller et ses collègues (2015) met d'ailleurs en valeur la validité externe de cette technique, réfutant ainsi la critique qu'en raison de sa nature imaginaire, les vignettes de cas ne

peuvent prédire les réelles réactions des participants. D'autre part, les vignettes de cas amoindrissent les risques de biais de désirabilité sociale, car les questions sont circonscrites à des mises en situation et non aux expériences de vie des participants (Alexander et Becker, 1978). En bref, les vignettes de cas donnent au chercheur la flexibilité nécessaire pour capturer avec fiabilité les subtilités d'un enjeu donné.

Cela dit, le nombre de vignettes de cas s'accroît rapidement à fur et à mesure que des variables sont ajoutées et il peut devenir difficile de rassembler un échantillon qui conserve une bonne puissance statistique (Auspurg et Hinz, 2015). Sinon, faire lire et réagir plusieurs mises en situation aux participants recrutés peut entraîner un biais d'attrition dans l'échantillonnage (Alexander et Becker, 1978 ; Atzmüller et Steiner, 2010). En ce qui concerne l'étude ci-présente, le modèle de la victime « idéale » implique cinq dimensions différentes (victime « fragile », projet « respectable », victime « irréprochable », contrevenant « inconnu », contrevenant « imposant ») (Christie, 1986 ; Hopkins, 2016), donc un total de 10 variables dichotomisées et $2^5 = 32$ vignettes de cas. Par conséquent, les variables intégrées dans les vignettes de cas doivent être choisies judicieusement afin d'éviter les enjeux méthodologiques susmentionnés. Les vignettes de cas de ce projet de recherche incorporent donc que les dimensions « fragile », « respectable » et « irréprochable » de la victime « idéale », celles-ci ayant reçu un soutien empirique grâce à l'analyse de Lewis et *al*. (2019) en lien avec les descriptions populaires de la victime. Cette démarche donne un total de 3 variables indépendantes dichotomisées, soit une quantité de $2^3 = 8$ vignettes de cas pouvant être distribuées au public à l'étude. Les variables indépendantes associées à chacune de ces trois dimensions (décrites en détail dans une section ultérieure) s'inspirent de la façon dont Hopkins (2016) a conceptualisé les qualités de l'entreprise victime « idéale ». Plus précisément, l'entreprise victime « irréprochable » concerne le commerce doté d'une bonne posture de cyber-résilience. L'entreprise victime « fragile » implique la PME, celle-ci suscitant de la sympathie en vertu de ses ressources limitées à prévenir la criminalité. L'entreprise victime « respectable » aborde plutôt le caractère moral inhérent au crime : un vol de données ayant touché les données non financières d'un nombre limité de clients devrait susciter moins d'indignation morale envers l'entreprise victime qu'un vol ayant touché les données financières d'un grand nombre de clients.

Participants

L'échantillon assujetti à l'expérience se compose essentiellement d'étudiants universitaires du premier cycle issus de l'Université de Montréal (UdeM), l'Université du Québec à Montréal (UQAM), l'Université Laval et l'Université du Québec à Trois-Rivières (UQTR). Quelques-uns sont des étudiants d'échange. Dans tous les cas, le seul critère d'exclusion de l'expérience a été que le participant ait au moins 18 ans. Les participants n'ont tiré aucun avantage financier ou autre de l'étude. La phase de recrutement et de participation s'est principalement déroulée durant les périodes de classe, entre le 13 janvier 2021 et le 31 mars 2021. Une portion des étudiants a été sollicitée par courriel ou via leur portail étudiant, spécialement si les instructeurs de certains cours ne pouvaient se permettre à allouer du temps en classe pour le projet de recherche. Avec un échantillon initial de 792 participants, l'étude a exclu les individus n'ayant pas répondu à au moins une question du sondage portant explicitement sur leur réaction vis-à-vis la vignette de cas qui leur a été affecté. L'échantillon final comporte 664 personnes (468 femmes et 183 hommes) âgées de 18 à 66 ans ($\bar{x}$ = 22,69, M = 21, s = 5,42). La majorité est d'origine ethnique blanche (79,4 %) et la plupart détiennent en ce moment un diplôme collégial (71,1 %). Les étudiants proviennent de programmes variés, dont la criminologie, le droit, la sécurité et les études policières. Outre d'autres programmes de sciences humaines et sociales (psychologie, sociologie, science politique, etc.), d'autres étudiants sont en chimie, en génie industriel et en mathématiques. Les statistiques descriptives des participants sont résumées ci-dessous :

Tableau 2 : Statistiques descriptives des participants de l'étude

	N	**%**
Genre		
Homme	183	27,6 %
Femme	468	70,5 %
Autre	4	0,6 %
Aucune réponse	9	1,4 %
Ethnie		
Peuples autochtones	5	0,8 %
Asiatique	22	3,3 %
Noire	42	6,3 %
Blanche	527	79,4 %
Hispanique	11	1,7 %
Autre	39	5,9 %
Aucune réponse	18	2,7 %

Diplôme		
Aucun diplôme	2	0,3 %
Diplôme secondaire	38	5,7 %
Diplôme collégial	472	71,1 %
Diplôme baccalauréat	101	15,2 %
Diplôme de maîtrise	13	2 %
Diplôme de doctorat	1	0,2 %
Autre	25	3,8 %
Aucune réponse	12	1,8 %
Groupe d'âge		
18-24 ans	503	75,8 %
25-64 ans	112	16,9 %
65 ans et plus	1	0,2 %
Aucune réponse	48	7,2 %
Université		
UdeM	331	49,8 %
UQAM	52	7,8 %
Université Laval	179	27 %
UQTR	71	10,7 %
Autre	6	0,9 %
Aucune réponse	25	3,8 %
Programme d'étude		
Criminologie	234	35,2 %
Droit	67	10,1 %
Sécurité et études policières	55	8,3 %
Économie	31	4,7 %
Génie industriel	27	4,1 %
Administration	25	3,9 %
Sociologie	24	3,6 %
Communication	24	3,7 %
Science forensique	16	2,4 %
Psychologie	15	2,3 %
Autre	149	15,5 %
Aucune réponse	41	6,2 %

Limites des données

Le projet de recherche utilise un échantillon d'étudiants, une source de données populaire en sciences humaines (Peterson, 2001), mais qui fait l'objet de nombreux débats en ce qui a trait à la généralisation des résultats, car certains argumentent que la population étudiante est plus homogène que le public général ou encore qu'elle diffère de façon importante des non-étudiants sur plusieurs dimensions psychologiques et comportementales (Peterson, 2001 ; Hanel et Vione, 2016). Ceci pourrait expliquer pourquoi Gilmartin-Zena (1983), ayant eu recours à un échantillon

d'étudiants universitaires pour examiner la faute sur la victime, a lancé l'hypothèse que le phénomène serait davantage accentué dans un échantillon ne partageant pas nécessairement le même portrait socioéconomique. Par ailleurs, une grande portion des étudiants ayant été sollicités dans le cadre de ce projet de recherche pour exprimer leurs opinions par rapport aux vignettes de cas sont inscrits dans un programme de criminologie, et il est possible que certains d'entre eux aient déjà suivi un cours en victimologie. Une étude de Fox et Cook (2011) laisse présager que ces personnes seraient moins enclines à mettre la faute sur une victime que les autres, car ce cursus leur a permis de développer davantage leur perspective critique en lien avec le phénomène de la victimisation. En même temps, l'article en question concerne exclusivement la responsabilisation des victimes de violence conjugale, d'agression sexuelle et de violence physique. Le domaine de la victimologie s'étant traditionnellement focalisée sur la victimisation des individus (Hopkins, 2016), il est possible que le statut de victime des entreprises, spécialement dans les cas de brèches de données où elles ont des obligations formelles à l'égard de l'intégrité des renseignements personnels des parties prenantes (CPVPC, 2020b), demeure ambigu et que le cursus des étudiants ne biaise pas la réaction de ces derniers durant l'expérience (Australian Institute of Criminology, 2004).

Cela dit, la population étudiante demeure très accessible pour les chercheurs et reste parfaitement adaptée pour établir, selon Henry (2008), les premiers fondements d'une quelconque découverte empirique. Il ajoute qu'il est plus important pour ces études d'assurer leur reproductibilité plutôt que leur généralisabilité. Ainsi, les méthodes de ce projet de recherche portant sur la cyber-résilience, un concept n'ayant essentiellement connu qu'une attention conceptuelle (Dupont et al., 2020), peuvent constituer un premier élan empirique et être répliquées ultérieurement dans une autre étude, cette fois-là en utilisant un échantillon du public général.

Instruments de collecte de données

La cueillette de données a été principalement réalisée grâce à deux outils : des vignettes de cas (présentées à l'annexe 1) et un court sondage d'environ 10 minutes (présenté à l'annexe 2). Les vignettes de cas mettent en évidence deux entreprises de vente au détail fictives, dénommées *Boîte à prix* et *ÉchangeGros*, ayant été les victimes d'un vol de données. Les caractéristiques de la mise en situation varient systématiquement selon les trois dimensions du modèle de la victime

« idéale ». La variable indépendante principale se rapporte à la posture de cyber-résilience de l'entreprise et assimile la dimension « irréprochable » de la victime « idéale » (Hopkins, 2016). La description de la posture de cyber-résilience des firmes s'inspire des pratiques ayant été identifiées durant la revue de littérature de ce projet de recherche comme ayant un bienfait sur la résilience face à la réaction du public. Pour réitérer, Choi et *al.* (2016) soulignent les bienfaits réputationnels d'un avis immédiat, qui exprime du regret, et qui est transparent par rapport aux circonstances de la brèche. Ainsi, dans les vignettes de cas où *Boîte à prix* et *ÉchangeGros* sont munies d'une forte posture de cyber-résilience, celles-ci ont su rapidement mobiliser leurs capacités communicatives après détection de la brèche. Dans les mises en situation où *Boîte à prix* et *ÉchangeGros* sont dépeintes comme ayant une faible posture de cyber-résilience, celles-ci ont attendu deux mois après la détection de la brèche avant de l'annoncer publiquement.

Similairement à certaines des déclarations de brèches de données dans Jenkins et *al.* (2014), les entreprises dans la condition expérimentale « forte posture de cyber-résilience » annoncent avec regret la brèche à leurs parties prenantes. Celles dans la condition expérimentale « faible posture de cyber-résilience » ont plutôt adopté un style littéraire désinvolte. *Boîte à prix* et *ÉchangeGros* dans la condition « forte posture de cyber-résilience » ont d'ailleurs bien détaillé les circonstances du vol. À partir des recommandations de la CPVPC (2018), une entreprise qui souhaite maintenir la transparence sur les circonstances d'une brèche doit communiquer : (1) les organisations visées et leur rôle par rapport aux renseignements touchés ; (2) comment et pourquoi l'atteinte est-elle survenue ; (3) quand elle a été découverte ; (4) où elle a eu lieu dans l'infrastructure ; (5) qui pourrait avoir accès aux données compromises. Dans les vignettes de cas, les firmes avec une forte posture de cyber-résilience ont donné cette information et ont été décrites comme étant très communicatives sur les circonstances du vol de données. En revanche, les commerces avec une faible posture de cyber-résilience n'ont pas communiqué cette information et ont donc été caractérisés comme ayant été peu communicatifs sur les circonstances de la brèche.

De même, le CPVPC (2018) prescrit aux entreprises d'inclure dans l'avis une description des étapes que peuvent emprunter les particuliers touchés pour se protéger des préjudices pouvant découler de la brèche. De plus, il est important d'inclure des coordonnées pour les clients désirant obtenir des informations supplémentaires sur l'incident. Dans les vignettes de cas, les firmes avec

une forte posture de cyber-résilience ont fourni des renseignements sur les façons de se protéger contre la fraude à l'identité, et ont laissé ouvertes leurs chaînes de communication, au cas où le public aurait des questions. Inversement, *Boîte à prix* et *ÉchangeGros* dans la condition expérimentale « faible posture de cyber-résilience) ont fourni peu de précisions sur les façons de se protéger de la fraude à l'identité. De même, elles ont gardé fermées leurs chaînes de communication, empêchant ainsi les clients de poser des questions aux représentants des entreprises respectives.

Enfin, avoir eu en place des solutions pour prévenir les vols de données et le mésusage des données réduit les dommages réputationnels d'un vol de renseignements personnels (Knight and Nurse, 2020; Syed, 2019; Syed and Dhillon, 2015). Dans la condition expérimentale « forte posture de cyber-résilience », *Boîte à prix et ÉchangeGros* ont affirmé avoir fait preuve de diligence raisonnable, annonçant qu'elles ont eu en place des procédés et technologies complètes pour prévenir la cybercriminalité et qu'elles ont aussi des dispositions pour empêcher le mésusage des données en cas de compromission. Les firmes avec une faible posture de cyber-résilience ont été réticentes à partager des détails sur leur culture de sécurité, mais les sources médiatiques font savoir que leurs pratiques de prévention de la cybercriminalité sont lacunaires. Selon l'état des connaissances, une forte posture de cyber-résilience devrait atténuer la réaction du public après un vol de données (Choi et al., 2016 ; Gwebu et al., 2018 ; Muzatko et Bansal, 2018 ; Novak et Vilceanu, 2019 ; Ponemon, 2017 ; Romanosky et al., 2014 ; Rosati et al., 2019 ; Syed, 2019 ; Syed et Dhillon, 2015).

La taille de l'entreprise, représentant la dimension « fragile » de la victime « idéale » (Hopkins, 2016), est dichotomisée en « petite entreprise » et en « grande entreprise ». Selon Hopkins (2016), la victimisation d'un petit commerce devrait susciter une meilleure sympathie de la part du public que la victimisation d'une grande firme en raison de ses ressources limitées pour prévenir la criminalité, bien que les recherches demeurent non concluantes dans le cas des vols de données (Cavusoglu et al., 2004 ; Gatzlaff et McCullough, 2010 ; Malhotra et Malhotra, 2011 ; Rosati et al., 2019). Dans le cadre de cette étude, *Boîte à prix* est une petite entreprise et *ÉchangeGros* est une grande entreprise. La troisième variable indépendante, la sévérité du vol, reflète la dimension « respectable » de la victime « idéale » (Hopkins, 2016). Dans le contexte de

la victimisation des entreprises, une firme serait vue comme respectable si le crime suscite une indignation morale en faveur de la victime (Hopkins, 2016). Comme indiqué dans la revue de littérature, les vols de données ne sont pas des crimes qui exonèrent les entreprises de la responsabilisation (Abhishta et al., 2017 ; Andoh-Baidoo et al., 2010 ; Berezina et al., 2012 ; Cavusoglu et al., 2004 ; Garg et al., 2003 ; Valecha et al., 2017), mais la gravité de la réaction négative du public varie tout de même dépendamment de la sévérité de l'incident (Garg et al., 2003 ; Gatzlaff et McCullough, 2010 ; Kamiya et al., 2020 ; Malhotra et Malhotra, 2011 ; Miller et Angelis, 2018 ; Morse et al., 2011 ; Romanosky et al., 2014 ; Tweneboah-Kodua et al., 2018 ; Tweneboah-Kodua et al., 2020). Sur les vignettes de cas, la sévérité du vol est décrite soit comme un « vol ayant touché les données non financières d'un nombre limité de clients » ou un « vol ayant touché les données financières d'un grand nombre de clients ». Selon les écrits, le second élément devrait entraîner une plus grave réaction du public envers l'entreprise victime (Garg et al., 2003 ; Gatzlaff et McCullough, 2010 ; Kamiya et al., 2020 ; Malhotra et Malhotra, 2011 ; Miller et Angelis, 2018 ; Morse et al., 2011 ; Romanosky et al., 2014 ; Tweneboah-Kodua et al., 2018 ; Tweneboah-Kodua et al., 2020).

Le cœur du sondage se caractérise sinon de six variables dépendantes liées au concept plus large de la réaction du public. Celles-ci se tirent des attitudes et des comportements soulevés dans la revue de littérature (Ablon et al., 2016 ; Choi et al., 2016, Kim et al., 2019 ; Romanosky et al., 2014 ; Syed, 2019 ; Syed et Dhillon, 2015 ; Valecha et al., 2017). Pour répondre au premier objectif spécifique (« Déterminer l'impact d'une posture de cyber-résilience sur les attitudes du public à l'égard des entreprises après un vol de données »), les trois premières variables à l'étude se rapportent à la dimension attitudinale de la réaction du public, les items respectifs étant représentés à l'aide d'une échelle Likert à 7 éléments. Tout d'abord, une variable porte sur le niveau de responsabilité accordé à *Boîte à prix* ou *ÉchangeGros* (faute) : « Je pense que le vol de données est la faute de l'entreprise » (1 = tout à fait d'accord à 7 = pas du tout d'accord). La deuxième variable concerne les sentiments envers la firme. Valecha et al. (2017) montrent que les réactions affectives des parties prenantes envers une brèche de données sont négatives, donc l'item dans le sondage adopte lui aussi une expression négative (sentiments négatifs) : « J'éprouve des sentiments négatifs à l'égard de l'entreprise » (1 = tout à fait d'accord à 7 = pas du tout d'accord). La croyance que *Boîte à prix* ou *ÉchangeGros* peut se remettre du vol de données fait le sujet de

la troisième variable (croyances négatives) : « Je pense que l'entreprise peut adéquatement surmonter ce nouveau défi » (1 = pas du tout d'accord à 7 = tout à fait d'accord). Le score dans ce cas a été inversé pour faciliter l'interprétation des résultats, avec un score de 1 signalant un pic de croyances négatives vis-à-vis l'entreprise victime.

Les trois prochaines variables concordent à la dimension comportementale de la réaction du public, les items étant également mesurés à l'aide d'une échelle Likert à 7 éléments. Celles-ci permettent de répondre au deuxième objectif spécifique (« Déterminer l'impact d'une posture de cyber-résilience sur les intentions comportementales du public à l'égard des entreprises après un vol de données »). La première variable porte sur le bouche-à-oreille positif : « Je dirai des commentaires positifs à propos de cette entreprise à mon entourage » (1 = tout à fait d'accord à 7 = pas du tout d'accord). La seconde variable traite sur l'intention d'achat : « Je continuerais de fréquenter cette entreprise » (1 = tout à fait d'accord à 7 = pas du tout d'accord). La variable finale porte attention sur les poursuites judiciaires : « J'intenterais un recours collectif contre l'entreprise si j'en avais le pouvoir » (1 = pas du tout d'accord à 7 = tout à fait d'accord). Encore une fois, le score du troisième item a été inversé pour simplifier les analyses, un score de 1 symbolisant cette fois un pic de comportements positifs envers la firme victime. L'ensemble des variables dépendantes permettent ultimement de tester le troisième objectif spécifique (« Établir l'association entre les attitudes et les intentions comportementales du public envers les entreprises après un vol de données »).

Sur le sondage, des variables démographiques ont été prises en compte à des fins de statistiques descriptives. Celles-ci incluent : (1) le genre du répondant (1 = Homme, 2 = Femme, 3 = Autre ; 9 = Aucune réponse) ; (2) l'âge du répondant ; (3) l'origine ethnique du répondant (1 = Peuples autochtones ; 2 = Asiatique ; 3 = Noire ; 4 = Blanche ; 5 = Hispanique ; 6 = Autre ; 9 = Aucune réponse) ; (4) le niveau d'éducation du répondant (1 = Pas de diplôme ; 2 = Secondaire ; 3 = Collégial ; 4 = Baccalauréat ; 5 = Maîtrise ; 6 = Doctorat ; 7 = Autre ; 9 = Aucune réponse) ; (5) l'université à laquelle le répondant est inscrit ; (6) son programme d'étude actuel. Les participants ont pu écrire leur adresse courriel à la fin du sondage au cas où ils souhaiteraient obtenir le sommaire des résultats de l'étude.

Procédure et modèle d'analyse

Un premier courriel a été envoyé à 45 instructeurs universitaires (40 % de l'UdeM ; 20 % de l'UQAM ; 24,4 % de l'Université Laval ; 15,6 % de l'UQTR) afin de leur demander la permission de présenter le projet de recherche à leur classe et de fournir dix minutes pour la participation à l'étude. Les courriels ont visé les cours de première année du baccalauréat en raison de leur grande taille de classe. Après une réponse positive, le second courriel décrit davantage l'objectif du projet de recherche, la procédure expérimentale envisagée ainsi que les réponses qui seraient capturées. Un total de 20 instructeurs ont répondu favorablement à la requête. Certains ont permis d'introduire le projet, mais non de laisser la participation lors des heures de cours en raison de contraintes dans le temps. Dans ce cas, les étudiants ont été priés de faire l'étude selon leurs disponibilités après le cours. Sinon, la grande majorité des enseignants ayant refusé la sollicitation ont tout de même accepté de faire une annonce de l'étude à leur classe par courriel ou via le portail étudiant de leur université respectif.

En raison des mesures de confinement dévouées à la lutte contre le COVID-19, les cours universitaires se sont déroulés à distance par l'entremise du logiciel de téléconférence *Zoom*. Lorsqu'un rendez-vous de recrutement a été établi par courriel, l'instructeur en question envoyait le lien URL vers la séance virtuelle avec la date et l'heure. Il suffisait de cliquer sur le lien à l'heure du rendez-vous pour joindre la classe. Après une brève mise en contexte de l'étude et des conditions de participation, les étudiants ont été invités à visiter un lien inséré sur la salle de clavardage de leur cours. Par ce lien, les volontaires ont donné leur consentement écrit avant de procéder à l'expérience en soi, où l'une des huit vignettes de cas (posture de cyber-résilience x taille de l'entreprise x sévérité du vol) leur a été assignée aléatoirement (voir le tableau 3 pour la distribution des vignettes de cas). Les questionnaires en ligne offrent certains avantages par rapport aux questionnaires papier-crayon. Une étude de Lucia et *al.* (2007) montre d'abord que les participants d'étude sont plus motivés à remplir des questionnaires Internet comparativement aux questionnaires papier-crayon en raison de la convivialité des interfaces numériques modernes. D'autre part, ils prennent moins de temps pour le terminer. Ceci est particulièrement pertinent pour ce projet de recherche, car les participants n'ont eu que dix minutes pour effectuer l'étude en classe. Les participants perçoivent aussi que les questionnaires en ligne protègent mieux la confidentialité de leurs informations et ils sont alors plus à l'aise de répondre à un questionnaire Internet qu'un

questionnaire papier-crayon. Enfin, Lucia et *al.* (2007) argumentent que les questionnaires Internet sont généralement moins coûteux. Dans le contexte de cette étude, les frais de transport ont été épargnés, ce qui a permis de rassembler davantage de personnes dans des régions extérieures de Montréal, soit Trois-Rivières et la ville de Québec. De même, les données recueillies en ligne peuvent être facilement exportées à un logiciel d'analyse statistique.

Tableau 3 : Distribution des vignettes de cas à l'étude

Vignettes de cas	**N**	**%**
(1) Petite entreprise — Vol de portée limitée/données non financières — Forte posture de cyber-résilience	91	13,7 %
(2) Petite entreprise — Vol de portée limitée/données non financières — Faible posture de cyber-résilience	84	12,7 %
(3) Grande entreprise — Vol de portée limitée/données non financières — Forte posture de cyber-résilience	80	12 %
(4) Grande entreprise — Vol de portée limitée/données non financières — Faible posture de cyber-résilience	92	13,9 %
(5) Petite entreprise — Vol de grande portée/données financières — Forte posture de cyber-résilience	83	12,5 %
(6) Petite entreprise — Vol de grande portée/données financières — Faible posture de cyber-résilience	90	13,6 %
(7) Grande entreprise — Vol de grande portée/données financières — Forte posture de cyber-résilience	82	12,3 %
(8) Grande entreprise — Vol de grande portée/données financières — Faible posture de cyber-résilience	62	9,3 %
Total	**664**	**100 %**

Après avoir lu la mise en situation, les participants ont répondu à des questions portant sur leurs attitudes et leurs intentions comportementales envers l'entreprise victime (*Boîte à prix* ou *ÉchangeGros*). L'étude s'est conclue avec les questions démographiques. Les étudiants ont sinon eu l'occasion d'inclure leur adresse courriel au cas où ils souhaiteraient recevoir le sommaire des résultats finaux après la rédaction du projet de recherche. Le jeu de données final a ensuite été transféré sur le logiciel d'analyse statistique *IBM SPSS Statistics 26* afin d'effectuer les analyses

quantitatives nécessaires pour déterminer l'impact d'une posture de cyber-résilience sur la réaction du public à la suite d'un vol de données chez les entreprises.

La réaction du public se divisant en dimension attitudinale et comportementale, le premier sous-objectif est de déterminer l'impact d'une posture de cyber-résilience sur les attitudes du public à l'égard des entreprises après un vol de données. Pour y répondre, des analyses multivariées de variance (MANOVA) ont été effectuées entre les trois premiers items du sondage (faute, sentiments négatifs et croyances négatives) et les variables indépendantes dépeintes sur les vignettes de cas (posture de cyber-résilience, taille de l'entreprise et sévérité du vol). Les tests MANOVA permettent aux chercheurs d'évaluer plusieurs variables dépendantes quantitatives en même temps et de déterminer si les variables indépendantes qualitatives ont un effet de façon individuelle (effet principal) et en combinaison les unes avec les autres (effet d'interaction) (Multivariate Analysis of Variance, s.d.). La MANOVA est donc utile pour les expériences employant des vignettes de cas parce que celles-ci cherchent souvent à mesurer les impacts de diverses combinaisons de variables sur un nombre donné de variables dépendantes (Alexander et Becker, 1978). Par exemple, il est possible que la posture de cyber-résilience d'une entreprise ne limite la réaction du public que pour les petites entreprises. Sinon, des tests ANOVA peuvent être réalisés après les tests MANOVA pour analyser les effets principaux significatifs du modèle, cette fois-ci en utilisant les variables dépendantes de manière individuelle (Institute for Digital Research and Education, 2021).

Les principes d'utilisation pour les tests MANOVA ont été majoritairement comblés, mais le test *M de Box* s'est avéré significatif pour le jeu de données. La trace de Pillai a donc été utilisée pour interpréter les tests statistiques. Les résultats du MANOVA permettent ultimement de répondre à la première hypothèse nulle de l'étude :

H^0a : La posture de cyber-résilience d'une entreprise touchée par un vol de données n'a pas d'impact sur les attitudes du public à son égard.

Le second sous-objectif est de mesurer l'impact d'une posture de cyber-résilience sur les intentions comportementales du public à l'égard des entreprises après un vol de données. Comme pour le premier sous-objectif, des tests MANOVA sont effectués entre les trois dernières variables

dépendantes (bouche-à-oreille positif ; intention d'achat ; et poursuites judiciaires) et les trois variables indépendantes de l'étude. Encore une fois, l'interprétation des résultats s'est faite grâce à la trace de Pillai. Ceci permet de rejeter ou non l'hypothèse nulle suivante :

> H^0b : La posture de cyber-résilience d'une entreprise touchée par un vol de données n'a pas d'impact sur les intentions comportementales du public à son égard.

Le troisième sous-objectif est d'établir l'association entre les attitudes et les intentions comportementales du public envers les entreprises après un vol de données. Afin de permettre les tests de corrélation, les variables indépendantes relatives aux attitudes, soit : (1) le niveau de responsabilité (faute) ; (2) les sentiments négatifs (sentiments négatifs) et (3) la croyance que l'entreprise se remettra de l'incident (croyances négatives) ont été regroupés dans une échelle de moyenne (α = .625) pour former un score moyen « d'attitudes négatives ». Un score de 1 indique un pic d'attitudes négatives envers l'entreprise, alors qu'un score de 7 signifie le contraire. Les variables dépendantes relèvent des items du sondage portant sur la dimension comportementale de la réaction du public, c'est-à-dire : (1) les commentaires positifs émis aux pairs à l'égard de la firme victime (bouche-à-oreille positif) ; (2) le niveau de fréquentation de l'entreprise après le vol (intention d'achat) et (3) l'intention de démarrer un recours collectif (poursuites judiciaires). Celles-ci ont constitué une échelle de moyenne (α = .668) dénommée « comportements favorables ». Cette fois-ci, un score de 1 signifie un pic de comportements favorables à l'égard de l'entreprise ; le contraire pour un score de 7. Les principes d'utilisation pour les tests de corrélation, incluant la distribution normale des variables et la linéarité des relations, sont comblés. Les résultats subséquents permettent de répondre à l'hypothèse nulle suivante :

> H^0c : Aucune association n'existe entre les attitudes négatives et les intentions comportementales favorables du public à la suite d'un vol de données.

Limites méthodologiques

Les décisions et autres compromis relatifs à la conception de cette étude impliquent quelques limites. En premier lieu, pour des raisons de faisabilité, l'étude n'a pas pu inclure dans son modèle d'analyse toutes les dimensions de la victime « idéale » (Christie, 1986) comme envisagé par Hopkins (2016). Il aurait été notamment pertinent d'examiner, relativement à l'« irréprochabilité » de la victime (posture de cyber-résilience), l'impact d'un contrevenant

« inconnu » (acteur externe vs menace interne) et celui d'un contrevenant « imposant » (techniques d'ingénierie sociale vs piratage informatique). Les recherches précédentes laissent présager qu'un employé malveillant usant de techniques d'ingénierie sociale (comme l'hameçonnage) pour voler les données d'une entreprise susciterait une plus grave réaction du public (Confente et al., 2019 ; Morse et al., 2011). En revanche, comme mentionnée précédemment, l'inclusion de ces deux dimensions aurait eu pour effet d'augmenter dramatiquement le nombre de vignettes de cas à distribuer. Afin de faire l'équilibre entre le montant de vignettes de cas et l'échantillon requis pour l'obtention de résultats fiables, le projet de recherche ci-présent a décidé de se focaliser sur les trois dimensions (victime « fragile », projet « respectable », victime « irréprochable ») ayant été prouvées comme étant saillantes dans les descriptions populaires des victimes (Lewis et al., 2019).

En second lieu, certains aspects des vignettes de cas ont été superficiellement abordés pour rendre ces dernières les plus brèves possibles et éviter ainsi un biais d'attrition dans l'échantillonnage. Il se peut cependant que certaines pratiques importantes de la cyber-résilience soient peu apparentes au lecteur alors qu'elles pourraient avoir un impact important sur leurs attitudes et intentions comportementales envers l'entreprise victime. Par ailleurs, les différentes actions entreprises par les firmes fictives après le vol de données ont été regroupées pour former un archétype dichotomique de posture de cyber-résilience. Autrement dit, il est possible que dans les cas réels de brèches d'informations, les commerces réagissent selon les meilleures pratiques dans certains aspects (comme annoncer rapidement qu'il y a eu brèche) mais ratent de combler d'autres enjeux communicatifs (comme ouvrir leurs chaînes de communication à toutes les parties prenantes), donnant alors lieu à une posture de cyber-résilience mitigée. Par exemple, Home Depot a manqué de sécuriser adéquatement ses points de vente, permettant à des attaquants de facilement les compromettre (Hawkins, 2015). De même, l'entreprise a été critiquée pour sa notification tardive de l'incident (Syed, 2019). En revanche, Home Depot a offert un abonnement gratuit de 12 mois à des services de protection d'identité, chose qui a éventuellement favorisé les comportements positifs des clients (comme l'intention d'achat) (Hoehle, 2021). Comme mentionné précédemment, ce choix méthodologique reflète le besoin d'assurer un nombre raisonnable de vignettes de cas pour l'échantillon envisagé.

CHAPITRE 3 — RÉSULTATS

Ce chapitre présente d'abord les analyses quantitatives qui permettent d'expliquer l'impact d'une posture de cyber-résilience sur la réaction du public à la suite d'un vol de données chez les entreprises. Les deux premières sous-sections utilisent des tests MANOVA et ANOVA afin d'expliquer respectivement l'impact de la cyber-résilience sur les (1) attitudes du public et sur les (2) intentions comportementales du public à l'égard des entreprises victimes. La troisième sous-section emploie des tests de corrélation pour déterminer s'il existe une association entre les attitudes et les intentions comportementales à l'étude.

Objectif spécifique 1 : L'impact d'une posture de cyber-résilience sur les attitudes du public à l'égard des entreprises après un vol de données

La dimension attitudinale de la réaction du public combine les trois variables dépendantes suivantes : (1) le niveau de responsabilité attribué à la firme victime dans la vignette de cas (faute) ; (2) les sentiments négatifs ressentis envers cette dernière (sentiments négatifs) et (3) la croyance que l'entreprise ne peut se remettre du vol de données (croyances négatives). Grâce à l'échelle Likert à 7 éléments utilisée pour le sondage, chacune des variables implique un score de 1 à 7. Un score de 1 signifie respectivement que le répondant met totalement la faute sur l'entreprise pour le vol, qu'il ressent des sentiments absolument négatifs envers celle-ci et qu'il maintient des croyances entièrement pessimistes sur la survie de l'entreprise. Un score de 7 pour chacune des trois variables signifie l'inverse. Le tableau 4 présente les moyennes de scores et les écarts-type des trois variables dépendantes selon (1) la posture de cyber-résilience de l'entreprise victime, (2) la taille de l'entreprise victime et (3) la sévérité du vol, donnant un total de huit conditions expérimentales.

Tableau 4 : Analyses univariées des attitudes du public envers la firme victime

	Faute (1 = Tout à fait d'accord à 7 = Tout à fait en désaccord)						Sentiments négatifs (1 = Tout à fait d'accord à 7 = Tout à fait en désaccord)						Croyances négatives (1 = Tout à fait en désaccord à 7 = Tout à fait d'accord)					
	Forte posture de cyber-résilience			Faible posture de cyber-résilience			Forte posture de cyber-résilience			Faible posture de cyber-résilience			Forte posture de cyber-résilience			Faible posture de cyber-résilience		
	n	***M***	***s***	***n***	***M***	***s***	***n***	***M***	***s***	***n***	***M***	***s***	***n***	***M***	***s***	***n***	***M***	***s***
Petite entreprise, Vol de portée limitée/données non financières	91	3.87	1.67	84	3.12	1.5	91	4.02	1.57	84	2.55	1.29	91	5.46	1.09	84	4.5	1.44
Petite entreprise, Vol de grande portée/données financières	82	4.07	1.76	90	3.14	1.47	82	4.11	1.61	90	2.46	1.14	82	5.29	1.36	90	4.41	1.56
Grande entreprise, Vol de portée limitée/données non financières	79	4.06	1.6	91	2.78	1.35	79	4.16	1.6	91	2.41	1.37	79	5.33	1.15	91	4.46	1,57
Grande entreprise, Vol de grande portée/données financières	82	3.65	1.64	62	3.13	1.59	82	3.76	1.50	62	2.37	1.35	82	5.45	0.96	62	4.55	1,62
Total	334	3.91	1.67	327	3.03	1.47	334	4.01	1.57	327	2.45	1.28	334	5.39	1.14	327	4.47	1.54

Le tableau 5 illustre les résultats des tests MANOVA permettant de répondre au premier objectif spécifique, soit de déterminer l'impact d'une posture de cyber-résilience sur les attitudes du public à l'égard d'une entreprise après un vol de données. Selon la trace de Pillai, il n'existe pas d'effet d'interaction à trois facteurs pour les attitudes du public (V = .006, F(3, 651) = 1.341, *η2 partiel* = .006, p > .05). De même, aucune interaction à deux facteurs ne subsiste entre les variables indépendantes et les variables dépendantes combinées relatives aux attitudes du public (taille de la firme x posture de cyber-résilience : V = .000, F(3, 651) = .034, *η2 partiel* = .000, p > .05 ; sévérité du vol x posture de cyber-résilience : V = .002, F(3, 651) = .483, *η2 partiel* = .002, p > .05 ; taille de la firme x sévérité du vol : V = .004, F(3, 651) = .940, *η2 partiel* = .004, p > .05). D'autre part, ni la taille de la firme (V = .003, F(3, 651) = .616, *η2 partiel* = .003, p > .05) ni la sévérité du vol (V = .003, F(3, 651) = .639, *η2 partiel* = .003, p > .05) n'exerce d'effet principal sur les attitudes négatives du public. En revanche, les analyses soutiennent que la posture de cyber-résilience d'une entreprise victime de vol de données a un effet principal sur les attitudes négatives du public (V = .255, F(3, 651) = 74.126, *η2 partiel* = .255, p < .01), ce qui permet de rejeter l'hypothèse nulle H_0a.

Tableau 5 : Analyses MANOVA (trace de Pillai) des attitudes du public envers la firme victime

	V	***F***	***η2 partiel***	***p***
Posture de cyber-résilience	.255	74.126	.255	.000**
Taille de la firme	.003	0.616	.003	.605
Sévérité du vol	.003	0.639	.003	.590
Taille de la firme x Posture de cyber-résilience	.000	0.034	.000	.992
Sévérité du vol x Posture de cyber-résilience	.002	0.483	.002	.694
Taille de la firme x Sévérité du vol	.004	0.940	.004	.421
Taille de la firme x Sévérité du vol x Posture de cyber-résilience	.006	1.341	.006	.260

*$p < .05$; ** $p < .01$

À la lumière de l'effet principal exercé par la posture de cyber-résilience sur les attitudes du public, des tests ANOVA (tableau 6) ont été menés pour déterminer son impact sur les variables dépendantes, cette fois-ci prises de manière individuelle. La posture de cyber-résilience d'une entreprise ayant subi un vol de données prédit de façon modérée ($p < .01$, $\eta = .272$) le niveau de responsabilité qui lui est attribué. Plus spécifiquement, sur une échelle de 1 à 7, le public a moins tendance à mettre la faute sur une firme ayant été capable de mobiliser ses mesures de sécurité et de communication ($M = 3.92$, $s = 1.67$) comparativement à une organisation avec une pauvre posture de cyber-résilience ($M = 3.03$, $s = 1.47$). La cyber-résilience a sinon un très fort impact ($p < .01$, $\eta = .479$) sur les sentiments négatifs ressentis à l'égard de l'entreprise. Autrement dit, une

bonne posture de cyber-résilience diminue les sentiments négatifs (M = 4.01, s = 1.57), relativement à une mauvaise posture de cyber-résilience (M = 2.45, s = 1.28). De même, elle prédit fortement ($p < .01$, $\eta = .320$) les croyances liées à la capacité d'une entreprise à rebondir des chocs causés par le vol de données. Plus précisément, une bonne posture de cyber-résilience limite les croyances pessimistes liées au futur de la firme (M = 5.38, s = 1.14) comparativement à une faible posture de cyber-résilience (M = 4.47, s = 1.54).

Tableau 6 : Analyses ANOVA des attitudes du public envers la firme victime

	Posture de cyber-résilience (FORTE et FAIBLE)			**FORTE**			**FAIBLE**		
	F	*η*	*p*	*M*	*s*	*n*	*M*	*s*	*n*
Faute	52.701	.272	.000**	3.92	1.67	336	3.03	1.47	327
Sentiments négatifs	195.904	.479	.000**	4.01	1.57	334	2.45	1.28	327
Croyances négatives	75.265	.320	.000**	5.38	1.14	336	4.47	1.54	327

*$p < .05$; ** $p < .01$

En somme, la qualité « irréprochable » de l'entreprise victime semble être la seule dimension du modèle de la victime « idéale » qui importe en ce qui a trait au premier objectif spécifique. Peu importe les circonstances du vol de données, toute entreprise, qu'elle soit de grande taille ou une PME, doit préparer et mobiliser ses capacités de prévention, de détection et de réponse à la cybercriminalité pour assurer sa résilience face aux attitudes négatives du public après un vol de renseignements personnels.

Objectif spécifique 2 : L'impact d'une posture de cyber-résilience sur les intentions comportementales du public à l'égard des entreprises après un vol de données

Les trois variables dépendantes de la dimension comportementale de la réaction du public combinent (1) les commentaires positifs émis aux pairs à l'égard de la firme victime dans la vignette de cas (bouche-à-oreille positif), (2) le niveau de fréquentation de l'entreprise après le vol (intention d'achat) et (3) l'intention de démarrer un recours collectif (poursuites judiciaires). Comme pour le volet attitudinal, chacune de ces variables se caractérise d'un score de 1 à 7. En revanche, un score de 1 pour chaque item signifie cette fois-ci que le répondant dirait que des

commentaires positifs à ses pairs à propos de la firme victime, que son niveau de fréquentation de l'entreprise resterait inchangé, et qu'il n'intenterait d'aucune façon un recours collectif s'il en avait le pouvoir. Un score de 7 pour chacune des variables indique l'inverse. Le tableau 7 illustre les moyennes de scores et les écarts-types des trois variables selon les trois variables indépendantes à l'étude, c'est-à-dire : (1) la posture de cyber-résilience de l'entreprise victime, (2) la taille de l'entreprise victime et (3) la sévérité du vol, donnant huit conditions expérimentales.

Tableau 7 : Analyses univariées des intentions comportementales du public envers la firme victime

	Bouche-à-oreille positif (1 = Tout à fait d'accord à 7 = Tout à fait en désaccord)						Intention d'achat (1 = Tout à fait d'accord à 7 = Tout à fait en désaccord)						Poursuites judiciaires (1 = Tout à fait en désaccord à 7 = Tout à fait d'accord)					
	Forte posture de cyber-résilience			Faible posture de cyber-résilience			Forte posture de cyber-résilience			Faible posture de cyber-résilience			Forte posture de cyber-résilience			Faible posture de cyber-résilience		
	n	***M***	***s***	***n***	***M***	***s***	***n***	***M***	***s***	***n***	***M***	***s***	***n***	***M***	***s***	***n***	***M***	***s***
Petite entreprise, Vol de portée limitée/données non financières	91	4.12	1.09	82	5.22	1.18	91	3.41	1.19	82	4.82	1.38	91	3.01	1.69	82	3.74	1.68
Petite entreprise, Vol de grande portée/données financières	83	4.19	1.28	90	5.29	1.24	83	3.47	1.44	90	4.73	1.47	83	3.01	1.71	90	3.74	1.85
Grande entreprise, Vol de portée limitée/données non financières	80	4.23	1.17	88	5.3	1.28	80	3.46	1.28	88	4.68	1.5	80	2.94	1.69	88	3.84	1.51
Grande entreprise, Vol de grande portée/données financières	82	4.34	1.16	59	5.54	1.28	82	3.73	1.43	59	5.17	1.39	82	3.13	1.55	59	4.05	1.79
Total	336	4.22	1.17	319	5.32	1.24	336	3.51	1.34	319	4.82	1.45	336	3.02	1.66	319	3.83	1.7

Les tests MANOVA sur le tableau 8 permettent de répondre au second objectif spécifique. Comme pour la dimension attitudinale, il n'existe pas d'effet d'interaction à trois facteurs (V = .001, $F(3, 645)$ = .253, *η2 partiel* = .001, $p > .05$) ni à deux facteurs (taille de la firme x posture de cyber-résilience : V = .001, $F(3, 645)$ = .186, *η2 partiel* = .001, $p > .05$; sévérité du vol x posture de cyber-résilience : V = .000, $F(3, 645)$ = .038, *η2 partiel* = .000, $p > .05$; taille de la firme x sévérité du vol : V = .005, $F(3, 645)$ = 1.165, *η2 partiel* = .005, $p > .05$) entre les variables indépendantes et les intentions comportementales du public à l'égard de l'entreprise victime. Par ailleurs, la taille de la firme et la sévérité du vol n'amènent pas d'effet principal ($p > .05$). En contrepartie, les analyses montrent un effet principal entre la posture de cyber-résilience d'une entreprise victime de vol de données et les comportements du public (V = .226, $F(3, 645)$ = 62.929, *η2 partiel* = .226, $p < .01$), ce qui permet de rejeter l'hypothèse nulle H_0b.

Tableau 8 : Analyses MANOVA (trace de Pillai) des intentions comportementales du public envers la firme victime

	V	***F***	***η2 partiel***	***p***
Posture de cyber-résilience	.226	62.929	.226	.000**
Taille de la firme	.005	0.986	.005	.399
Sévérité du vol	.005	1.035	.005	.377
Taille de la firme x Posture de cyber-résilience	.001	0.186	.001	.906
Sévérité du vol x Posture de cyber-résilience	.000	0.038	.000	.990
Taille de la firme x Sévérité du vol	.005	1.165	.005	.322
Taille de la firme x Sévérité du vol x Posture de cyber-résilience	.001	0.253	.001	.859

*$p < .05$; ** $p < .01$

Les tests ANOVA (tableau 9) révèlent plus précisément un fort lien entre la cyber-résilience et les commentaires positifs relégués aux pairs par rapport à une entreprise ($p < .01$, $\eta = .397$). Ainsi, le public dirait davantage à leur entourage des commentaires positifs à propos de l'entreprise si cette dernière a une forte posture de cyber-résilience ($M = 4.22$, $s = 1.17$) que si elle a une faible posture de cyber-résilience ($M = 5.28$, s = 1.29). D'autre part, une forte relation ($p <$

.01, η = .425) existe entre la cyber-résilience et le niveau de fréquentation chez une entreprise victime. Le public serait plus enclin à visiter une entreprise se munissant d'une forte posture de cyber-résilience (M = 3.51, s = 1.34) comparativement à celle ayant démontré une pauvre posture de cyber-résilience (M = 4.82, s = 1.45). Enfin, la cyber-résilience a un impact modéré sur l'intention de démarrer des poursuites judiciaires (p < .01, η = .234), avec une forte posture de cyber-résilience réduisant les intentions de poursuites (M = 3.02, s = 1.66), relativement à une faible posture de cyber-résilience (M = 3.83, s = 1.7). En bref, comme pour le premier sous-objectif, une entreprise doit se rendre « irréprochable » à l'aide d'une forte posture de cyber-résilience pour minimiser la gravité des intentions comportementales négatives du public après un vol de données, et ce, même si elle comble les dimensions « fragile » et « respectable » de la victime « idéale ».

Tableau 9 : Analyses ANOVA des intentions comportementales du public envers la firme victime

	Posture de cyber-résilience (FORTE et FAIBLE)			**FORTE**			**FAIBLE**		
	F	*η*	*p*	*M*	*s*	*n*	*M*	*s*	*n*
Bouche-à-oreille positif	123.705	.397	.000**	4.22	1.17	336	5.28	1.29	326
Intention d'achat	145.039	.425	.000**	3.51	1.34	336	4.82	1.45	325
Poursuites judiciaires	37.998	.234	.000**	3.02	1.66	336	3.83	1.70	323

*p < .05 ; ** p < .01

Objectif spécifique 3 : L'association entre les attitudes et les intentions comportementales du public envers les entreprises après un vol de données

Pour cette partie de l'étude, des tests de corrélation ont été effectués entre les variables liées au volet attitudinal de la réaction du public et celles de la dimension comportementale. D'une part, les items relatifs aux attitudes (faute, sentiments négatifs et croyances négatives) ont été regroupés dans une échelle de moyenne (α = .625) dénommée « attitudes négatives ». De même, les items se rapportant aux intentions comportementales (bouche-à-oreille positif, intention d'achat et poursuites judiciaires) ont été réunis dans une échelle de moyenne (α = .668) appelée « intentions comportementales favorables ».

Les tests de corrélation révèlent une très forte relation linéaire négative entre les attitudes négatives et les intentions comportementales favorables du public à l'égard d'une entreprise victime de vol de données (r = -.656, p < .01). En d'autres mots, plus une personne a d'attitudes négatives envers une firme ayant subi un vol de données, moins elle aurait tendance à agir favorablement envers elle (dire des comportements positifs, continuer à le fréquenter ou s'abstenir d'intenter des poursuites judiciaires). Ces résultats permettent de rejeter l'hypothèse nulle H_0c du projet de recherche et n'appuient conséquemment pas l'argument du *privacy paradox* (Barnes, 2006 ; Martin et al., 2020). D'autre part, ils indiquent que les dommages réputationnels causés par un vol de données peuvent avoir des implications pour la survie d'une entreprise touchée. Le tableau 10 résume les résultats en lien avec le troisième objectif spécifique :

Tableau 10 : Tests de corrélation entre les attitudes et les intentions comportementales du public

	M	***s***	**Attitudes (*r*)**	**Comportements (*r*)**
Attitudes	3.89	1.19	1	-.656**
Comportements	4.1	1.20	-.656**	1

*p < .05 ; ** p < .01

CHAPITRE 4 — DISCUSSION

Comme déjà mentionné, la plupart des travaux actuels en lien avec la cyber-résilience s'attardent sur sa définition, ses principes et la façon dont elle devrait idéalement se manifester au sein des organisations (Dupont et al., 2020). Comme il existe peu d'articles explicatifs au sujet des pratiques de cyber-résilience, les bienfaits d'une posture de cyber-résilience par rapport à la sévérité des incidents de cybersécurité demeurent implicites. Ainsi, les vols de données peuvent impliquer une réaction négative du public certes, mais il est possible que ce soit la manière dont une entreprise gère l'incident qui pourrait ultimement décider la résilience de celle-ci face à ces dégâts de nature réputationnelle (Abhishta et al., 2017 ; Andoh-Baidoo et al., 2010 ; Berezina et al., 2012 ; Cavusoglu et al., 2004 ; Garg et al., 2003 ; Knight et Nurse, 2020 ; Valecha et al., 2017).

L'objectif principal du projet de recherche ci-présent a donc été d'expliquer l'impact d'une posture de cyber-résilience sur la réaction du public à la suite d'un vol de données chez les entreprises. À la lumière des réactions identifiées lors de la revue de littérature, l'étude a divisé la réaction du public en un volet attitudinal et comportemental pour donner lieu à deux premiers objectifs spécifiques, soit d'expliquer l'impact d'une posture de cyber-résilience sur les (1) attitudes et les (2) intentions comportementales du public vis-à-vis les entreprises touchées par un vol d'informations (Ablon et al., 2016 ; Choi et al., 2016, Kim et al., 2019 ; Romanosky et al., 2014 ; Syed, 2019 ; Syed et Dhillon, 2015 ; Valecha et al., 2017). Le projet de recherche a aussi tenté de comprendre l'association entre les attitudes et les intentions comportementales du public à l'égard des entreprises victimes de vol de données.

À l'aide du modèle de la victime « idéale » adaptée pour les entreprises (Hopkins, 2016), une étude expérimentale à base de vignettes de cas a été effectuée afin de mesurer les attitudes ainsi que les intentions comportementales du public par rapport à une entreprise victime de vol de données, et ce, selon la qualité « irréprochable » de celle-ci. Les pratiques de cyber-résilience identifiées durant la revue de littérature comme ayant un bienfait sur la réaction du public ont été incorporées dans cette dimension de la victime « idéale » pour donner matière à la variable indépendante principale « posture de cyber-résilience » (Choi et al., 2016 ; Gatzlaff et McCullough, 2010 ; Gwebu et al., 2018 ; Jenkins et al., 2014 ; Knight et Nurse, 2020 ; Muzatko et Bansal, 2018 ; Ponemon, 2017 ; Syed, 2019 ; Syed et Dhillon, 2015). Les dimensions « fragile » (taille de l'entreprise : petite entreprise vs. grande entreprise) et « respectable » (sévérité du vol :

vol de portée limitée/données non financières vs. vol de grande portée/données financières) ont également été prises en compte dans le modèle d'analyse.

Retour sur les résultats principaux

Pour réitérer, le premier objectif spécifique a été d'expliquer l'impact d'une posture de cyber-résilience sur les attitudes du public à l'égard des entreprises ayant subi un vol de données. Les analyses statistiques révèlent qu'une bonne posture de cyber-résilience limite les attitudes négatives du public, comparativement à une mauvaise posture de cyber-résilience. Plus spécifiquement, elle amoindrit le niveau de responsabilité attribué envers la firme victime concernée, la gravité des sentiments négatifs entretenus à l'égard de celle-ci et les croyances pessimistes sur la capacité de l'entreprise à surmonter adéquatement les défis posés par l'incident. Le deuxième objectif s'est voulu de déterminer l'impact d'une posture de cyber-résilience sur les intentions comportementales du public par rapport aux entreprises ayant subi un vol de données. Comme pour le volet attitudinal, les résultats indiquent que, relativement à une mauvaise posture de cyber-résilience, une bonne posture de cyber-résilience favorise les comportements positifs du public à l'endroit d'un commerce touché par un vol de données. Le public aurait davantage tendance à dire des commentaires positifs à leurs pairs à propos de la firme, à continuer de fréquenter cette dernière et à ne pas intenter de poursuites judiciaires.

En somme, les résultats appuient l'observation que des procédés et des technologies de sécurité robustes ainsi que des mécanismes de communication de crise efficaces limitent la sévérité de la réaction du public (Choi et al., 2016 ; Gwebu et al., 2018 ; Muzatko et Bansal, 2018 ; Novak et Vilceanu, 2019 ; Ponemon, 2017 ; Romanosky et al., 2014 ; Rosati et al., 2019 ; Syed, 2019 ; Syed et Dhillon, 2015). Plus théoriquement, la dimension « irréprochable » de la victime « idéale » permet à une entreprise de mieux revendiquer un statut de victime pour le vol de données (Hopkins, 2016). Elle signale un engagement envers la protection des données des parties prenantes, chose que le public attend des organisations à tout instant (Berezina et al., 2012 ; Gemalto, 2018 ; Syed, 2019). Plusieurs implications théoriques et pratiques (décrites dans la prochaine sous-section) découlent de cette affirmation.

En contrepartie, les analyses n'ont pu établir de lien entre la taille de la firme et les attitudes de même que les comportements du public. L'état des connaissances rapporte des résultats mitigés au sujet de l'impact de la taille de l'entreprise sur la réaction du public après une brèche de données : certains auteurs argumentent qu'elle est moins sévère si le vol s'est déroulé au sein d'une PME comparée à une grande entreprise, alors que d'autres affirment le contraire (Cavusoglu et al., 2004 ; Gatzlaff et McCullough, 2010 ; Malhotra et Malhotra, 2011 ; Rosati et al., 2019). Il est possible que l'étude expérimentale ne puisse appuyer l'une ou l'autre de ces interprétations parce qu'inclure la posture de cyber-résilience dans le modèle d'analyse pourrait supplanter le rôle maintenu par la taille de l'entreprise sur la réaction du public après un vol de données. En d'autres mots, une vignette de cas qui omettrait toutes les dimensions de la victime « idéale » à l'exception de la victime « fragile » pourrait certes montrer qu'une petite entreprise a plus ou moins de facilité à revendiquer le statut de victime après un vol de données, mais ce serait sûrement en raison du manque d'informations sur la façon dont elle a agi avant, pendant et après l'incident de cybersécurité. Les travaux antérieurs ayant traité de l'impact de la taille de l'entreprise sur la réaction négative du public ont examiné des cas réels de brèches d'informations sans toutefois tenir compte de la manière dont les PME ou les grandes entreprises à l'étude ont mobilisé leurs capacités de sécurité et de communication après un incident (Cavusoglu et al., 2004 ; Gatzlaff et McCullough, 2010 ; Malhotra et Malhotra, 2011 ; Rosati et al., 2019). Il se peut que les firmes à l'étude aient eu des postures de cyber-résilience différente les unes des autres, ce qui a mené à des résultats contradictoires avec l'expérience ci-présente en lien avec l'impact de la taille de l'entreprise sur la réaction du public après une brèche d'informations. Il se peut que les résultats n'aient pu montrer d'association entre la sévérité du vol et la réaction du public pour cette même raison, et ce, même si les connaissances passées affirment que les fuites de renseignements affectant les données financières d'un grand nombre de particuliers exacerbent la réaction négative du public (Gatzlaff et McCullough, 2010 ; Garg et al., 2003 ; Kamiya et al., 2020 ; Malhotra et Malhotra, 2011 ; Miller et Angelis, 2018 ; Morse et al., 2011 ; Romanosky et al., 2014 ; Tweneboah-Kodua et al., 2018, Tweneboah-Kodua et al., 2020). Plus précisément, il est possible que ce ne soit pas tant la sévérité du vol qui a eu un impact sur la réputation des firmes dans ces études que la façon dont celles-ci ont abordé la cyber-résilience au sein de leur organisation. L'étude ci-présente tient compte de ce facteur dans le modèle d'analyse.

Cela dit, il peut être contradictoire de constater que la sévérité du vol n'a pas d'impact sur la réaction du public à la suite d'un vol de données alors que les solutions de détection en cybersécurité cherchent justement à déclencher le plan de réponse aux incidents avant que l'incident en question prenne inutilement de l'ampleur (Cichonski et al., 2012 ; ISO, 2020). Cependant, ceci ne veut pas dire que la détection des incidents est inutile pour la cyber-résilience à la réaction négative du public après une brèche d'informations confidentielles. Comme souligné par l'ISO (2020), un vol de données peut autant être détecté par la chaîne d'approvisionnement de l'organisation que par une partie tierce externe telle que les médias. Ainsi, Beldad et al., (2018) montrent que le public réagirait mieux par rapport à une entreprise si celle-ci est la première à les informer d'un incident quelconque. Par exemple, des clients de Home Depot ont culpabilisé celle-ci pour la brèche en son sein parce que la firme ne l'a publiquement déclaré qu'après sa détection par un expert de sécurité externe. Une entreprise devrait donc s'assurer d'être la première à détecter et annoncer au public la brèche de donnée pour favoriser sa résilience face aux dommages réputationnels (Knight et Nurse, 2020). Dans cette étude, il est présumé que la firme victime a été la première à détecter le vol de données. Les mesures de réponse décrite sur chacune des vignettes de cas font ensuite l'objet de sa posture de cyber-résilience (« faible » ou « forte »).

Enfin, les observations découlant de l'étude ne peuvent confirmer s'il existe une interaction entre la taille de l'entreprise, la sévérité du vol et la posture de cyber-résilience sur les attitudes et les intentions comportementales du public à l'égard de l'entreprise victime. En tenant compte des autres résultats, ceci veut ultimement signifier que peu importe la sévérité du vol (la nature des renseignements personnels et l'étendue du vol) et la taille de l'entreprise, la posture de cyber-résilience aura le même impact sur la gravité des dégâts réputationnels (les autres variables indépendantes n'étant pas significatifs). Ceci rentre en ligne avec les attentes des parties prenantes où toutes les entreprises doivent être les gardiens des données clients et protéger celles-ci de toute intrusion (Bentley et al., 2018 ; Choi et al., 2016 ; Malhotra et Malhotra, 2011). Une firme avec une mauvaise posture de cyber-résilience brime de façon flagrante les attentes en question et invite donc des dommages réputationnels pour elle-même (Malhotra et al., 2017). Par conséquent, toute entreprise ayant subi un vol de données quelconque devrait immédiatement lancer un avis public et indiquer qu'elle avait des mesures adéquates pour prévenir la brèche et sinon le mésusage des données, avec les certifications indépendantes pour le prouver (Cole, 2016 ; Gwebu et al., 2018 ;

Miller et Angelis, 2018 ; Ponemon, 2017 ; Syed, 2019 ; Syed et Dhillon, 2015). D'autre part, il est important qu'elle communique de façon transparente les circonstances de la brèche (qui est visé, comment et pourquoi la brèche a eu lieu, où elle a eu lieu, qui peut avoir accès à ces informations, etc.) (Choi et al., 2016 ; CPVPC, 2020 ; Gatzlaff et McCullough, 2010 ; Jenkins et al., 2014). Enfin, elle devrait relayer au public les façons de se protéger de la fraude à l'identité et laisser ouvertes ses chaînes de communications afin de permettre le dialogue avec les personnes désirant avoir un suivi des événements.

Le troisième objectif spécifique a examiné le lien entre les attitudes et les intentions comportementales du public à l'égard d'une firme victime de vol de données. Le phénomène du *privacy paradox* soutient qu'il existe une contradiction entre les attitudes et les comportements des utilisateurs face à leurs renseignements personnels (Barnes, 2006). Plus précisément, même si la majorité des utilisateurs se disent préoccupés par les enjeux de vie privée, ils font très peu pour protéger leurs données personnelles. Dans le contexte de la réaction du public à la suite d'un vol de données, Martin et *al.* (2020) notent par l'entremise d'une étude expérimentale que les particuliers auront moins tendance à faire affaire avec une autre personne si cette dernière trahit leur confiance en matière de protection de la vie privée. Les auteurs concluent ainsi qu'il n'y a pas de *privacy paradox* parce que les particuliers changent leurs habitudes de consommation envers les firmes pour lesquelles ils considèrent les responsables en matière de protection des données. Les résultats de l'étude ci-présente appuient les résultats de Martin et al. (2020) : les attitudes envers la firme victime de vol de données sont reliées aux intentions comportementales à son égard. Plus le public maintient des attitudes négatives, moins il agit favorablement vis-à-vis l'entreprise. Ce constat laisse aussi présager que les dommages réputationnels suscités par les vols de données impliquent une perturbation de nature économique sur le commerce en question. À la lumière des autres résultats, une posture de cyber-résilience peut limiter l'impact de ces chocs.

Cela dit, même si cette étude n'observe pas le phénomène du *privacy paradox* en ce qui a trait aux habitudes des consommateurs, ceci ne veut pas dire qu'il rejette entièrement le concept. En premier lieu, il est important de noter que l'étude mesure les intentions comportementales et non les comportements réels des particuliers. Un individu peut dire qu'il ne fréquenterait plus une entreprise si cette dernière a manqué de prévenir et de répondre à un vol de données, mais ceci ne

veut pas nécessairement dire qu'il le fera réellement. Le *privacy paradox* pourrait donc subsister de cette façon. D'autre part, les lois sur la déclaration obligatoire des brèches de données cherchent à inciter les individus à se protéger des préjugés d'une fuite, mais l'état des connaissances montre que malgré les préoccupations du public par rapport à la compromission de leurs informations et à la fraude à l'identité, peu vont adopter des mesures de protection individuelles, et ce, peu importe leur situation socioéconomique (Ablon et al., 2016 ; LastPass, 2020 ; Piquero et al., 2011 ; Ponemon, 2014 ; Salesforce, 2018 ; Zou et al., 2018). Les particuliers ont plutôt tendance à donner cette responsabilité aux entreprises et de punir celles qui manquent à ce devoir (Gemalto, 2018 ; Berezina et al., 2012). Par surcroît, les résultats du troisième objectif spécifique du projet de recherche ci-présent ne peuvent conclure si la déclaration du vol de données dans la mise en situation motive les particuliers à entamer des démarches de protection contre les crimes pouvant découler d'une brèche de renseignements personnels.

Implications théoriques

Les résultats émanant des deux premiers objectifs spécifiques de l'étude impliquent que parmi les dimensions de la victime « idéale », seule la qualité « irréprochable » de la victime importe dans le contexte des vols de données. Ceci veut dire que les entreprises jouissent d'un certain niveau d'agentivité parce que les dimensions qui sont hors de leur contrôle immédiat après les faits, notamment leur taille (qualité « fragile » de la victime) et la sévérité du vol (qualité « respectable » de la victime), ne déterminent pas leur position dans la hiérarchie de la victime « idéale ». En revanche, il devient plus facile pour une organisation de revendiquer un statut de victime si elle est capable de mobiliser adéquatement ses capacités de réponse après la détection d'un vol de données. Cela dit, il est impossible de confirmer si une firme peut réellement être une victime « idéale » aux yeux du public après un vol de données. Une entreprise victime de vol d'informations n'a nécessairement pas pu prévenir la brèche et, tous éléments confondus, ceci provoque un certain niveau de dommages réputationnels en raison de la violation des attentes du public par rapport à la protection des données (Abhishta et al., 2017 ; Andoh-Baidoo et al., 2010 ; Berezina et al., 2012 ; Cavusoglu et al., 2004 ; Garg et al., 2003 ; Knight et Nurse, 2020 ; Valecha et al., 2017). Dans le cadre de cette étude expérimentale, une victime « idéale » aurait techniquement un score de 7 pour chacun des items dans le volet attitudinal pour souligner une absence d'attitudes négatives du public à son égard et un score de 1 pour les items de la dimension

comportementale pour indiquer une présence absolue d'intentions comportementales favorables vis-à-vis elle. Même Hopkins (2016) avoue dans son modèle de la victime « idéale » que les entreprises risquent de ne jamais jouir du même statut de victime que ce que les individus peuvent obtenir. Quoi qu'il en soit, ce projet de recherche peut conclure que la qualité « irréprochable » d'une organisation ayant subi un vol de données permettrait à celle-ci d'occuper une meilleure position dans la hiérarchie de la victime « idéale », mais n'assure pas le statut complet de victime. La définition de la cyber-résilience présuppose effectivement que les incidents de cybersécurité provoqueront toujours des chocs réputationnels pour l'organisation concernée et qu'une forte posture de cyber-résilience (la qualité « irréprochable » de la victime) ne peut espérer que de les limiter et éventuellement de les surmonter (Bryson, 2018).

Implications pratiques

Pour réitérer, une bonne posture de cyber-résilience permet de réduire la gravité de la réaction négative du public à la suite d'un vol de données. La taille de l'entreprise et la sévérité du vol ne montrent quant à elles aucun impact, donc toute entreprise devrait mobiliser ses mesures de prévention, de détection de même que de réponse aux incidents, et ce, peu importe les circonstances de la brèche. Conséquemment, même les petites entreprises avec un budget limité pour les enjeux de sécurité doivent faire preuve d'un certain engagement si elles espèrent rebondir adéquatement des dégâts réputationnels causés par un vol d'informations.

Il existe plusieurs cadres et modèles de meilleures pratiques pour prévenir, détecter et répondre aux incidents de cybersécurité, bien que peu se réfèrent explicitement aux PME et à leurs diverses contraintes économiques (Cyber Security Coalition, s.d. ; Cichonski et al., 2012 ; ISO, 2020 ; Morreale, 2008 ; NCSC, 2020 ; NIST, 2018). Afin de déployer une stratégie rentable, mais efficace de cyber-résilience face aux dégâts réputationnels après un vol de données, les PME doivent plus que jamais identifier les systèmes et les actifs contenant les informations personnelles de ses clients pour ensuite les chiffrer (Cyber Security Coalition, s.d. ; Gouvernement du Canada, 2021 ; NCSC, 2020). Effectuer la vigie des menaces principales vis-à-vis la compromission de ces données permet ensuite d'implanter une gamme de contrôles adaptés à l'écosystème numérique présent (Cyber Security Coalition, s.d. ; NIST, 2018). Comme noté précédemment, l'hameçonnage constitue la menace principale vis-à-vis les données clients, et les mesures de sécurité devraient

être ajustées en conséquence (Aleroud et Zhou, 2017 ; Alsharnouby et al., 2015 ; Arachchilage et al., 2016 ; Carella et al., 2017 ; Maynes, 2019 ; Proofpoint, 2020 ; Sheng et al., 2007 ; Verizon, 2021 ; Wen et al., 2019). L'entreprise pourrait ensuite être capable d'argumenter au public qu'elle a fait preuve de diligence raisonnable en matière de prévention des brèches d'informations et de mésusage des données (Gwebu et al., 2018 ; Knight et Nurse, 2020). La mise en place de solutions de détection gratuites ou du moins sous-traitées permet de réduire les coûts en ce qui a trait à l'identification d'une brèche au sein de la PME (Carìas et al., 2018 ; Cichonski et al., 2012 ; Detken et al., 2015 ; Kent et al., 2016). Après avoir documenté le confinement et l'éradication de l'incident, la PME sera capable de décrire au public les circonstances de la brèche ainsi que les façons de se protéger des risques qui pourraient en découler (CIO Strategy Council, 2021 ; Choi et al., 2016 ; Cyber Security Coalition, s.d. ; Jenkins et al., 2014). Elle aura ensuite l'occasion de présenter ses excuses et d'ouvrir le dialogue avec le public. Enfin, la PME pourra toujours organiser une éventuelle séance de « leçons apprises » dans les quelques semaines qui suivent l'incident afin d'améliorer les mesures de prévention, de détection et de réponse existantes dans l'infrastructure (CIO Strategy Council, 2021).

À la lumière de ces différentes recommandations, une entreprise de toute taille peut prendre en main sa cyber-résilience face à la réaction du public après un vol de données. Les parties prenantes en bénéficieraient aussi parce qu'une bonne posture de cyber-résilience de la part de l'entreprise mitige les risques de mésusage de leurs données (Gwebu et al., 2018 ; Knight et Nurse, 2020) et elle implique aussi un meilleur suivi par rapport à l'intégrité de leurs données au fil du temps (Choi et al., 2016).

Limites des résultats de l'étude

Plusieurs limites découlent des conclusions soulevées de cette étude expérimentale. Tout d'abord, la posture de cyber-résilience de *Boîte à prix* et de *ÉchangeGros*, même si décrite de façon concise, formait la grande partie du contenu dans les vignettes de cas. Il serait donc possible que cet élément de la mise en situation ait été plus saillant dans les pensées des participants que la taille de l'entreprise ou la sévérité du vol, ces deux dernières variables étant comprises dans une même phrase. Les résultats pourraient donc sous-estimer l'impact de la taille de l'entreprise et de la sévérité du vol sur la réaction du public. Une étude expérimentale future pourrait examiner le

rôle de ces variables dans le niveau des dommages réputationnels en l'absence de la cyber-résilience et tester ainsi que les dimensions « fragile » et « respectable » du modèle de la victime « idéale ». Toutefois, la validité externe pourrait en souffrir, car une entreprise répond adéquatement à un vol de données ou sa réponse laisse à désirer pour le public (Syed, 2019 ; Syed et Dhillon, 2015). Un modèle d'analyse qui ne tient pas compte des actions (ou leur absence) de la firme prises en lien avec un vol de renseignements risque d'omettre une partie importante de la variance.

Dans un deuxième temps, les résultats ne peuvent prédire la durée de la réaction du public après un vol de données, seulement qu'elle existe et qu'une posture de cyber-résilience est capable de le limiter. Il serait donc pertinent d'effectuer une étude de type longitudinale pour combler cette limite dans l'état des connaissances. Il serait possible qu'une posture de cyber-résilience permette à une entreprise de rebondir plus rapidement des dommages de nature réputationnelle, chose qui n'a pas été analysée dans ce projet (Ponemon, 2017).

Une troisième limite concerne l'opérationnalisation de la variable indépendante principale « posture de cyber-résilience ». Les pratiques de cyber-résilience ayant été incluses dans les vignettes de cas s'inspirent des recommandations prouvées comme ayant un impact favorable sur la résilience à l'égard des dommages de nature réputationnels après un vol de données (Choi et al., 2016 ; Gatzlaff et McCullough, 2010 ; Gwebu et al., 2018 ; Jenkins et al., 2014 ; Muzatko et Bansal, 2018 ; Ponemon, 2017 ; Syed, 2019 ; Syed et Dhillon, 2015). Celles-ci ne seraient donc pas nécessairement applicables pour les chocs physiques, psychologiques ou sociaux que peuvent aussi provoquer les fuites de renseignements ou les incidents de cybersécurité en général. Par exemple, l'Enquête canadienne sur la cybersécurité et le cybercrime (Statistics Canada, 2018) montre que les incidents de cybersécurité bouleversent fréquemment la productivité des organisations. Même si les pratiques examinées dans ce projet de recherche font bel et bien partie d'un plan complet de cyber-résilience dans les entreprises, les praticiens doivent s'appuyer sur d'autres travaux pour implanter des mesures qui favoriseraient davantage leur résilience face à l'ensemble des incidents de cybersécurité.

Une quatrième limite implique le fait que ce projet de recherche est une étude expérimentale, ce qui veut nécessairement dire que les variables de la cyber-résilience, la taille de l'entreprise et la sévérité du vol sont manipulées au sein d'un milieu artificiel. La vraie vie se compose de nombreux autres facteurs pouvant obscurcir l'impact de la cyber-résilience sur la réaction du public après un vol de données. D'une part, il est possible que les entreprises ne suivent pas à la lettre les meilleures pratiques de cyber-résilience et commettent des erreurs au cours de la gestion de l'incident. Par exemple, elles peuvent avoir immédiatement lancé un avis après la déclaration de l'incident, certes, mais omettre de faire le suivi transparent des événements avec le public. L'exécution d'un plan de réponse peut aussi prendre une mauvaise tournure, que ce soit à cause du niveau de compétence du personnel ou de toute autre raison inattendue, d'où la pertinence d'une séance de « leçons apprises » après les événements de la cyberattaque (CIO Strategy Council, 2021). Les vignettes de cas dans le cadre de cette étude ne mesurent d'ailleurs que les intentions comportementales des participants et non leurs comportements réels. Comme déjà mentionné, une personne pourrait dire qu'elle agirait d'une certaine façon envers une organisation sans toutefois que ce soit réellement le cas. De plus, certaines entreprises sont tout simplement des géants dans le marché (comme Facebook dans le monde des réseaux sociaux ou Amazon dans le monde du *e-commerce*) et leur présence éminente dans la conscience des consommateurs peut supplanter toute forme de choc réputationnel causé par un vol d'informations ainsi que de sa gestion subséquente (Gwebu et al., 2018). Ainsi, il se peut que les intentions comportementales des particuliers relevées dans la présente étude (bouche-à-oreille positif ; intention d'achat ; poursuites judiciaires) ne reflètent pas les comportements observés sous ces conditions, sinon que pour une courte durée pour une entreprise donnée (Acquisti et al., 2006 ; Avery, 2021 ; Ko et Dorantes, 2006). À la lumière de ces possibilités, les recherches futures pourraient examiner davantage les bienfaits d'une posture de cyber-résilience sur la réaction du public après un vol de données chez des entreprises réelles. Ces recherches devraient aussi envisager d'utiliser des échantillons non-étudiantes, car la présente étude n'a usé qu'un échantillon étudiant pour en arriver à ses conclusions et ceci a pour effet de limiter la généralisation des résultats (Peterson, 2001 ; Hanel et Vione, 2016).

Une dernière limite concerne le troisième objectif spécifique (« Établir l'association entre les attitudes et les intentions comportementales du public envers les entreprises après un vol de

données »). Bien qu'une association ait été démontrée entre les attitudes et les intentions comportementales du public envers les entreprises après un vol de données, il est important de noter que les participants ont été influencés par les vignettes de cas, ce qui pourrait avoir un effet sur les résultats par la suite. Il serait pertinent d'examiner l'association sans que les participants soient confrontés à une mise en situation de vol de données au moment du sondage.

CONCLUSION

Les brèches de données frappant de plus en plus l'imaginaire collectif, de nombreux pays industrialisés, dont le Canada, ont mis en vigueur des lois qui obligent les entreprises à déclarer publiquement ces incidents (Zou et al., 2019). Bien que Ces dispositions juridiques tentent d'encourager l'adoption individuelle de mesures de protection contre la fraude à l'identité, les particuliers préfèrent déléguer la tâche de sécurité des données aux entreprises qui hébergent leurs informations (Ablon et al., 2016 ; Gemalto, 2018 ; Ping Identity, 2019). Les firmes qui manquent de prévenir les fuites de renseignements personnelles briment donc les attentes de leurs parties prenantes et risquent de subir une réaction négative du public (Malhotra et al., 2017). Ces dommages de nature réputationnelle peuvent éventuellement représenter une menace existentielle pour l'entreprise s'ils ne sont pas contrôlés (Knight et Nurse, 2020). Les facteurs atténuants de cette réaction étant pourtant peu explorés, ce projet de recherche se veut un premier regard empirique sur le rôle que peut jouer une posture de cyber-résilience dans la réaction du public après un vol de données. L'emploi du modèle de la victime « idéale » (Hopkins, 2016) permet de déterminer dans quelle mesure une entreprise peut revendiquer un statut de victime par l'entremise de sa posture de cyber-résilience (victime « irréprochable »). La taille de l'entreprise (victime « fragile ») et la sévérité du vol (victime « respectable ») ont également été prises en compte dans les analyses en raison des travaux empiriques antérieurs sur la victime « idéale » (Lewis et al., 2019) et des articles se rapportant à leur impact par rapport à la réaction du public (Cavusoglu et al., 2004 ; Gatzlaff et McCullough, 2010 ; Garg et al., 2003 ; Kamiya et al., 2020 ; Malhotra et Malhotra, 2011 ; Miller et Angelis, 2018 ; Romanosky et al., 2014 ; Rosati et al., 2019 ; Tweneboah-Kodua et al., 2018 ; Tweneboah-Kodua et al., 2020). Ainsi, une étude expérimentale à base de vignettes de cas utilisant les trois dimensions susmentionnées a été effectuée à l'aide d'un échantillon final de 664 personnes. Celles-ci ont lu une vignette de cas, sur laquelle figure une entreprise victime de vol de données ayant soit une forte posture de cyber-résilience ou une faible posture de cyber-résilience. Les participants ont ensuite répondu à un court sondage portant sur leurs attitudes et leurs intentions comportementales vis-à-vis l'entreprise en question.

Les analyses montrent que la posture de cyber-résilience d'une entreprise a un impact sur la réaction du public après un vol de données. Les résultats de cette étude permettent de faire l'affirmation que les facteurs qui sont hors de portée immédiate de l'entreprise après l'incident (la taille de l'entreprise et la sévérité du vol) ne déterminent pas leur statut de victime. Ceci est de bon

augure pour les organisations privées parce qu'elles peuvent bel et bien prendre en main leur cyber-résilience face à la réaction du public après un vol de données. Ce faisant, les particuliers peuvent jouir d'une meilleure transparence de la part de l'entreprise et d'une meilleure protection de leurs données. En somme, bien que les commerces, peu importe leur posture de cyber-résilience, ne doivent pas s'attendre à être complètement déresponsabilisés d'un vol de données, ils peuvent tout de même agir de sorte à limiter les dégâts réputationnels et économiques sous-jacents.

Les recherches futures pourraient examiner la pertinence des autres dimensions de la victime « idéale » n'ayant pas été abordées par l'étude expérimentale ci-présente (le contrevenant « imposant » et « inconnu »), car les recherches sont d'accord pour dire respectivement que la méthode d'attaque et la provenance de l'attaque ont un impact sur la réaction du public après une brèche de renseignements (Andoh-Baidoo et al., 2010 ; Confente et al., 2019 ; Morse et al., 2011). Encore une fois, l'attention serait dirigée ici sur les fuites de nature criminelle. Une autre étude pourrait alors essayer de montrer si une posture de cyber-résilience minimise la réaction du public de la même façon dans les cas accidentels, comparativement aux incidents de type criminel. Enfin, d'autres travaux empiriques pourraient tester l'impact de certaines pratiques de cyber-résilience sur d'autres chocs provoqués par les incidents de cybersécurité, comme ceux par rapport à la productivité d'une entreprise. Les pistes de recherche susmentionnées pourraient certainement employer une approche expérimentale basée sur des vignettes de cas et utiliser un échantillon non-étudiant pour renforcer la généralisation des résultats. En revanche, il pourrait également être pertinent d'évaluer un jeu de données d'incidents de cybersécurité réels et leur gestion subséquente afin d'explorer les comportements réels des clients au lieu de leurs intentions comportementales.

RÉFÉRENCES

Abhishta, Joosten, R. et Nieuwenhuis, L. J. M. (2017). *Analysing the impact of a DDoS attack announcement on victim stock prices*. 2017 25th Euromicro International Conference on Parallel, Distributed and Network-based Processing, Saint-Pétersbourg, Russie. 10.1109/PDP.2017.82

Ablon, L., Heaton, P., Lavery, D. et Romanosky, S. (2016). *Consumer attitudes toward data breach notifications and loss of personal information*. RAND Corporation. 10.7249/RR1187

Accenture. (2018). *The nature of effective defense: shifting from cybersecurity to cyber resilience*. Accenture. https://www.accenture.com/_acnmedia/accenture/conversion-assets/dotcom/documents/local/en/accenture-shifting-from-cybersecurity-to-cyber-resilience-pov.pdf

Acquisti, A., Friedman, A. et Telang, R. (2006). *Is there a cost to privacy breaches? An event study*. Twenty-Seventh International Conference on Information Systems, Milwaukee, WI, États-Unis. https://aisel.aisnet.org/icis2006/94/?utm_source=aisel.aisnet.org%2Ficis2006%2F94&utm_medium=PDF&utm_campaign=PDFCoverPages

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S. et Upton, D. (2018). A taxonomy of cyber-harms: defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1), 1-15. 10.1093/cybsec/tyy006

Ajzen, I. et Fishbein, M. (1978). Attitude-behavior relations: A theoretical analysis and review of empirical research. *Psychological Bulletin*, *84*(5), 888-918. https://doi.org/10.1037/0033-2909.84.5.888

Aleroud, A. et Zhou, L. (2017). Phishing environments, techniques, and countermeasures: a survey. *Computers & Security*, *68*, 160-196. 10.1016/j.cose.2017.04.006

Alexander, C. S. et Becker, H. J. (1978). The use of vignettes in survey research. *The Public Opinion Quarterly*, *42*(1), 93-104. https://doi.org/10.1086/268432

Alexius, K. (2020). The exposed child in a qualitative study of cases at the Swedish Schools Inspectorate. An ideal or not-so-ideal victim? *Pedagogy, Culture & Society*, *28*(3), 367-382. https://doi.org/10.1080/14681366.2019.1649296

Alsharnouby, M., Alaca, F. et Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies*, *82*, 69-82. 10.1016/j.ijhcs.2015.05.005

Amir, M. (1968). Victim precipitated forcible rape. *Journal of Criminal Law and Criminology*, *58*(4), 493-502. https://scholarlycommons.law.northwestern.edu/jclc/vol58/iss4/4

Anderson, R., Barton, C., Böhme, R., Clayton, R., Gañán, C., Grasso, T., … Vasek, M. (2019). *Measuring the changing cost of cybercrime*. The 18th Annual Workshop on the Economics of Information Security, Boston, MA, États-Unis. 10.17863/CAM.41598

Andoh-Baidoo, F. K., Amoako-Gyampah, K. et Osei-Bryson, K.-M. (2010). How internet security breaches harm market value. *IEEE Security Privacy*, *8*(1), 36-42. 10.1109/MSP.2010.37

Arachchilage, N. A. G., Love, S. et Beznosov, K. (2016). Phishing threat avoidance behaviour: an empirical investigation. *Computers in Human Behavior*, *60*, 185-197. 10.1016/j.chb.2016.02.065

Atzmüller, C. et Steiner, P. M. (2010). Experimental vignette studies in survey research. *Methodology: European Journal of Research Methods for the Behavioral and Social Sciences*, *6*(3), 128-138. 10.1027/1614-2241/a000014

Auspurg, K. et Hinz, T. (2015). Setting up the experimental design. Dans Auspurg, K. et Hinz, T. (dir.), *Factorial Survey Experiments* (p. 16-59). SAGE Publications Inc. 10.4135/9781483398075.n3

Austin, L., Liu, B. F. et Jin, Y. (2012). How audiences seek out crisis information: exploring the social-mediated crisis communication model. *Journal of Applied Communication Research*, *40*(2), 188-207. 10.1080/00909882.2012.654498

Australian Institute of Criminology. (2004). *Crimes against business: a review of victimisation, predictors and prevention.* Australian Institute of Criminology. https://www.aic.gov.au/sites/default/files/2020-05/tbp011.pdf

Avery, A. (2021). After the disclosure: measuring the short-term and long-term impacts of data breach disclosures on the financial performance of organizations. *Information & Computer Security*, *ahead-of-print*(publication électronique avant impression). https://doi.org/10.1108/ICS-10-2020-0161

Ayala, E. E., Kotary, B. et Hetz, M. (2018). Blame attributions of victims and perpetrators: effects of victim gender, perpetrator gender, and relationship. *Journal of Interpersonal Violence*, *33*(1), 94-116. 10.1177/0886260515599160

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, *11*(9). https://doi.org/10.5210/fm.v11i9.1394

Beigi, G., Hu, X., Maciejewski, R. et Liu, H. (2016). An overview of sentiment analysis in social media and Its applications in disaster relief. Dans W. Pedrycz et S.-M. Chen (dir.), *Sentiment analysis and ontology engineering: an environment of computational*

intelligence (p. 313-340). Springer International Publishing. 10.1007/978-3-319-30319-2_13

Beldad, A. D., van Laar, E. et Hegner, S. M. (2018). Should the shady steal thunder? The effects of crisis communication timing, pre-crisis reputation valence, and crisis type on post-crisis organizational trust and purchase intention. *Journal of Contingencies and Crisis Management*, *26*(1), 150-163. https://doi.org/10.1111/1468-5973.12172

Bentley, J. M., Oostman, K. R. et Shah, S. F. A. (2018). We're sorry but it's not our fault: Organizational apologies in ambiguous crisis situations. *Journal of Contingencies and Crisis Management*, *26*(1), 138-149. 10.1111/1468-5973.12169

Berezina, K., Cobanoglu, C., Miller, B. L. et Kwansa, F. A. (2012). The impact of information security breach on hotel guest perception of service quality, satisfaction, revisit intentions and word-of-mouth. *International Journal of Contemporary Hospitality Management*, *24*(7), 991-1010. 10.1108/09596111211258883

Berger, R. J. et Searles, P. (1985). Victim-offender interaction in rape: victimological, situational, and feminist perspectives. *Women's Studies Quarterly*, *13*(3/4), 9-15. https://www.jstor.org/stable/25164241

Bhagavatula, S., Bauer, L. et Kapadia, A. (2020). *(How) do people change their passwords after a breach?*. IEEE Signal Processing Workshop, Rio de Janeiro, Brésil. https://www.ieee-security.org/TC/SPW2020/ConPro/papers/bhagavatula-conpro20.pdf

Bhamra, R., Dani, S. et Burnard, K. (2011). Resilience: the concept, a literature review and future directions. *International Journal of Production Research*, *49*(18), 5375-5393. 10.1080/00207543.2011.563826

Billings, A. B., Crumbley, D. L. et Knott, C. L. (2021). Tangible and intangible costs of white-collar crime. *Journal of Forensic and Investigative Accounting*, *13*(2), 288-301. http://web.nacva.com.s3.amazonaws.com/JFIA/Issues/JFIA-2021-No2-3.pdf

Bilodeau, H., Lari, M. et Uhrbach, M. (2019). *Les défis des entreprises canadiennes quant à la cybersécurité et au cybercrime, 2017*. Statistique Canada. https://www150.statcan.gc.ca/n1/pub/85-002-x/2019001/article/00006-fra.htm

Bisogni, F. (2016). Proving limits of state data breach notification laws: is a federal law the most adequate solution? *Journal of Information Policy*, *6*, 154-205. 10.5325/jinfopoli.6.2016.0154

Boes, S. et Leukfeldt, E. R. (2017). Fighting cybercrime: a joint effort. Dans R. M. Clark et S. Hakim (dir.), *Cyber-physical security: protecting critical infrastructure at the state and local level* (p. 185-203). Springer International Publishing. 10.1007/978-3-319-32824-9_9

Bossler, A. M. et Berenblum, T. (2019). Introduction: new directions in cybercrime research. *Journal of Crime and Justice*, *42*(5), 495-499. 10.1080/0735648X.2019.1692426

Boyd, B., Bergh, D. et Ketchen, D. (2010). Reconsidering the reputation—performance relationship: a resource-based view. *Journal of Management*, *36*(3), 588-609. 10.1177/0149206308328507

Bryson, R. (2018). *Building cyber resilience*. The Conference Board of Canada 2018, Ottawa, ON, Canada. https://www.conferenceboard.ca/temp/1236a7e2-ac3f-441f-bf97-d5883dc30128/9822_Building%20Cyber%20Resilience_BR_FR.pdf

Burnes, D., DeLiema, M. et Langton, L. (2020). Risk and protective factors of identity theft victimization in the United States. *Preventive Medicine Reports*, *17*, 1-8. 10.1016/j.pmedr.2020.101058

Carella, A., Kotsoev, M. et Truta, T. M. (2017). *Impact of security awareness training on phishing click-through rates*. 2017 IEEE International Conference on Big Data, Boston, MA, États-Unis. 10.1109/BigData.2017.8258485

Carìas, J. F., Labaka, L., Sarriegi, J. M. et Hernantes, J. (2018). *An approach to the modeling of cyber resilience management*. 2018 Global Internet of Things Summit, Bilbao, Espagne. https://doi.org/10.1109/GIOTS.2018.8534579

Cavusoglu, H., Mishra, B. et Raghunathan, S. (2004). The effect of internet security breach announcements on market value: capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, *9*(1), 69-104. 10.1080/10864415.2004.11044320

Centre antifraude du Canada. (2021). *Vol d'identité et fraude à l'identité*. Gouvernement du Canada. https://www.antifraudcentre-centreantifraude.ca/scams-fraudes/identity-identite-fra.htm

Chapple, M. et Seidl, D. (2021). *CompTIA Security+ Study Guide* (8e éd.). Sybex.

Chen, H., Chiang, R. H. L. et Storey, V. C. (2012). Business intelligence and analytics: from Big Data to big impact. *MIS Quarterly*, *36*(4), 1165-1188. 10.2307/41703503

Choi, B. C. F., Kim, S. S. et Jiang, Z. (Jack). (2016). Influence of firm's recovery endeavors upon privacy breach on online customer behavior. *Journal of Management Information Systems*, *33*(3), 904-933. 10.1080/07421222.2015.1138375

Christie, N. (1986). The ideal victim. Dans M. Duggan (eds.), *Revisiting the 'ideal victim': developments in critical victimology* (p. 11-23). Policy Press. 10.1007/978-1-349-08305-3_2

Cichonski, P., Millar, T., Grance, T. et Scarfone, K. (2012). *Computer security incident handling guide : recommendations of the National Institute of Standards and Technology*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

CIO Strategy Council. (2021). *CAN/CIOSC 104*. CIO Strategy Council. https://ciostrategycouncil.com/standards/public-review/can-ciosc-104/

Clement, J. (2020). *Number of social media users worldwide*. Statista. https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

Coffey, J. W. (2019). Difficulties in determining data breach impacts, *Journal of Systemics, Cybernetics and Informatics*, *17*(5), 9-13. http://www.iiisci.org/journal/sci/FullText.asp?var=&id=IP069LL19

Cohen, M. A. (2013). *Economic costs of white-collar versus street crime*. American Association for the Advancement of Science 2013 Annual Meeting, Boston, MA, États-Unis. https://www.researchgate.net/publication/267541922_Economic_Costs_of_White-Collar_Versus_Street_Crime

Cole, B. (2016). Five reasons to invest in ISO 27001 and other security certifications. TechTarget. https://searchcompliance.techtarget.com/blog/IT-Compliance-Advisor/Five-reasons-to-invest-in-ISO-27001-and-other-security-certifications

Confente, I., Siciliano, G. G., Gaudenzi, B. et Eickhoff, M. (2019). Effects of data breaches from user-generated content: a corporate reputation analysis. *European Management Journal*, *37*(4), 492-504. 10.1016/j.emj.2019.01.007

Coombs, W. T. (2007). Protecting organization reputations during a crisis: the development and application of situational crisis communication theory. *Corporate Reputation Review*, *10*(3), 163-176. 10.1057/palgrave.crr.1550049

Coombs, W. T. (2010). Parameters for crisis communication. Dans W. T. Coombs et S. J. Holladay (eds.), *Handbook of crisis communication* (p. 17-53). Blackwell Publishing Ltd. 10.1002/9781444314885.ch1

Copes, H. et Vieraitis, L. M. (2009). Bounded rationality of identity thieves: using offender-based research to inform policy. *Criminology & Public Policy*, *8*(2), 237-262. 10.1111/j.1745-9133.2009.00553.x

Correia, I. et Vala, J. (2003). When will a victim be secondarily victimized? The effect of observer's belief in a just world, victim's innocence and persistence of suffering. *Social Justice Research*, *16*(4), 379-400. https://doi.org/10.1023/A:1026313716185

Cortina, L. M., Rabelo, V. C. et Holland, K. J. (2018). Beyond blaming the victim: toward a more progressive understanding of workplace mistreatment. *Industrial and Organizational Psychology*, *11*(1), 81-100. 10.1017/iop.2017.54

Cowan, G. (2000). Women's hostility toward women and rape and sexual harassment myths, *Violence Against Women*, *6*(3), 238-246. 10.1177/10778010022181822

CPVPC. (2018). *Ce que vous devez savoir sur la déclaration obligatoire des atteintes aux mesures de sécurité*. Commissariat à la protection de la vie privée du Canada. https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/protection-des-renseignements-personnels-pour-les-entreprises/mesures-de-securite-et-atteintes/atteintes-a-la-vie-privee/comment-reagir-a-une-atteinte-a-la-vie-privee-dans-votre-entreprise/gd_pb_201810/

CPVPC. (2019). *Un an après l'entrée en vigueur des déclarations obligatoires des atteintes à la protection des données : ce que nous avons appris et ce que les entreprises doivent savoir*. Commissariat à la protection de la vie privée du Canada. https://www.priv.gc.ca/fr/blogue/20191031/

CPVPC. (2020). *Loi sur la protection des renseignements personnels et les documents électroniques*. Commissariat à la protection de la vie privée du Canada. https://laws-lois.justice.gc.ca/pdf/P-8.6.pdf

Cromwell, P. et Thurman, Q. (2003). The devil made me do it: use of neutralizations by shoplifters. *Deviant Behavior*, *24*(6), 535-550. 10.1080/713840271

Cross, C. (2020). 'Oh we can't actually do anything about that': the problematic nature of jurisdiction for online fraud victims. *Criminology & Criminal Justice*, *20*(3), 358-375. 10.1177/1748895819835910

Cross, C., Parker, M. et Sansom, D. (2019). Media discourses surrounding 'non-ideal' victims: the case of the Ashley Madison data breach. *International Review of Victimology*, *25*(1), 53-69. 10.1177/0269758017752410

Cross, C., Richards, K. et Smith, R. G. (2016). *The reporting experiences and support needs of victims of online fraud*. Australian Institute of Criminology. https://www.aic.gov.au/publications/tandi/tandi518

CVE. (2021). *CVE data feeds*. Common Vulnerabilities and Exposures. https://cve.mitre.org/cve/data_feeds.html

Cyber Security Coalition (s.d.). *Cyber Security Incident Management Guide*. Cyber Security Coalition. https://www.cybersecuritycoalition.be/content/uploads/cybersecurity-incident-management-guide-EN.pdf

Detken, K., Rix, T., Kleiner, C., Hellmann, B. et Renners, L. (2015). *SIEM approach for a higher level of IT security in enterprise networks*. 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Varsovie, Polande. https://doi.org/10.1109/IDAACS.2015.7340752

Dharmapala, D., Garoupa, N. et McAdams, R. H. (2009). Belief in a just world, blaming the victim, and hate crime statutes. *Review of Law & Economics*, *5*(1), 311-345. https://doi.org/10.2202/1555-5879.1276

Dhillon, G. (2015). *What to do before and after a cybersecurity breach?*. Kogod School of Business. https://www.american.edu/kogod/research/cybergov/upload/what-to-do.pdf

Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. *Journal of Cybersecurity*, *5*(1), 1-17. 10.1093/cybsec/tyz013

Dupont, B., Shearing, C. et Bernier, M. (2020). *Withstanding cyber-attacks: cyber-resilience practices in the financial sector*. Global Risk Institute. https://globalriskinstitute.org/publications/withstanding-cyber-attacks-cyber-resilience-practices-in-the-financial-sector/

Finch, J. (1987). The vignette technique in survey research. *Sociology*, *21*(1), 105-114. 10.1177/0038038587021001008

Fisse, B. et Braithwaite, J. (1986). The allocation of responsibility for corporate crime: individualism, collectivism and accountability. *Sydney Law Review*, *11*(3), 468-513. https://heinonline.org/HOL/Page?handle=hein.journals/sydney11&div=36&g_sent=1&casa_token=&collection=journals

Fox, K. A. et Cook, C. L. (2011). Is knowledge power? The effects of a victimology course on victim blaming. *Journal of Interpersonal Violence*, *26*(17), 3407-3427. 10.1177/0886260511403752

Freedman, M. (2020). *How and why businesses collect consumer data*. Business News Daily. https://www.businessnewsdaily.com/10625-businesses-collecting-data.html

Gagnon, M.-A. (2020). *Projet de loi 64: Des sanctions de 25 M$ en cas de fuite de données personnelles*. Le Journal de Québec. https://www.journaldequebec.com/2020/06/12/projet-de-loi-64-des-sanctions-de-25-millions--en-cas-de-fuite-de-donnees-personnelles

Garg, A., Curtis, J. et Halper, H. (2003). Quantifying the financial impact of IT security breaches. *Information Management & Computer Security*, *11*(2), 74-83. 10.1108/09685220310468646

Gatzert, N. (2015). The impact of corporate reputation and reputation damaging events on financial performance: empirical evidence from the literature. *European Management Journal*, *33*(6), 485-499. 10.1016/j.emj.2015.10.001

Gatzlaff, K. M. et McCullough, K. A. (2010). The effect of data breaches on shareholder wealth. *Risk Management and Insurance Review*, *13*(1), 61-83. 10.1111/j.1540-6296.2010.01178.x

Gemalto. (2018). *Data Breaches & Customer Loyalty 2018*. Gemalto. http://octopi.com/pdf/customer-loyalty-report.pdf

Gendarmerie royale du Canada. (2020). *Le Groupe national de coordination contre la cybercriminalité (GNC3)*. Gendarmerie royale du Canada. https://www.rcmp-grc.gc.ca/fr/gnc3

Ghadge, A., Weiß, M., Caldwell, N. D. et Wilding, R. (2019). Managing cyber risk in supply chains: a review and research agenda. *Supply Chain Management: An International Journal*, *25*(2), 223-240. 10.1108/SCM-10-2018-0357

Gilmartin-Zena, P. (1983). Attribution theory and rape victim responsibility. *Deviant Behavior*, *4*(3-4), 357-374. 10.1080/01639625.1983.9967622

Gladly. (2019). *Customer Expectations Report: trends and insights from 1500 consumers about customer service*. Gladly. https://cdn2.hubspot.net/hubfs/2771217/2019%20Customer%20Expectations%20Reports/2019%20Customer%20Expectations%20Report.pdf

Gobert, J. J. (1977). Victim precipitation. *Columbia Law Review*, *77*(4), 511-553. 10.2307/1121822

Golla, M., Wei, M., Hainline, J., Filipe, L., Dürmuth, M., Redmiles, E. et Ur, B. (2018). *« What was that site doing with my Facebook password? »: designing password-reuse notifications*. Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, ON, Canada. 10.1145/3243734.3243767

Golladay, K. et Holtfreter, K. (2017). The consequences of identity theft victimization: an examination of emotional and physical health outcomes. *Victims & Offenders*, *12*(5), 741-760. 10.1080/15564886.2016.1177766

Goode, S., Hoehle, H., Venkatesh, V. et Brown, S. A. (2017). User compensation as a data breach recovery action: an investigation of the Sony PlayStation network breach. *MIS Quarterly*, *41*(3), 703–727. 10.25300/MISQ/2017/41.3.03

Gouvernement du Canada (2021). *Baseline Cyber Security Controls for Small and Medium Organizations V1.2*. Canadian Center for Cyber Security. https://cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations

Gouvernement du Canada. (2019). *Principales statistiques relatives aux petites entreprises - Novembre 2019 - Recherche et statistique sur la PME*. Gouvernement du Canada. https://www.ic.gc.ca/eic/site/061.nsf/fra/h_03114.html

Gouvernement du Canada. (2020). *Utilisation non autorisée d'ordinateur*. Gouvernement du Canada. https://laws-lois.justice.gc.ca/fra/lois/C-46/section-342.1.html

Gwebu, K. L., Wang, J. et Wang, L. (2018). The role of corporate reputation and crisis response strategies in data breach management. *Journal of Management Information Systems*, *35*(2), 683-714. 10.1080/07421222.2018.1451962

Hainmueller, J., Hangartner, D. et Yamamoto, T. (2015). Validating vignette and conjoint survey experiments against real-world behavior. *Proceedings of the National Academy of Sciences*, *112*(8), 2395-2400. 10.1073/pnas.1416587112

Hanel, P. H. P. et Vione, K. C. (2016). Do student samples provide an accurate estimate of the general public? *PLOS One*, *11*(12), 1-10. 10.1371/journal.pone.0168354

Hawkins, B. (2015). Case study: the Home Depot data breach. SANS Institute. https://sansorg.egnyte.com/dl/d82dKCwimy/?

Hayes, R. M., Lorenz, K. et Bell, K. A. (2013). Victim blaming others: rape myth acceptance and the just world belief. *Feminist Criminology*, *8*(3), 202-220. 10.1177/1557085113484788

Heidt, M., Gerlach, J. P. et Buxmann, P. (2019). Investigating the security divide between SME and large companies: how SME characteristics influence organizational IT security investments. *Information Systems Frontiers*, *21*(6), 1285-1305. https://doi.org/10.1007/s10796-019-09959-1

Helmkamp, J., Ball, R. et Townsend, K. (1996). *Definitional dilemma: can and should there be a universal definition of white collar crime?* Proceedings of the academic workshop, Morgantown, WV, États-Unis. https://www.ncjrs.gov/pdffiles1/Digitization/166244NCJRS.pdf

Henry, P. J. (2008). Student sampling as a theoretical problem. *Psychological Inquiry*, *19*(2), 114-126. 10.1080/10478400802049951

Hoehle, H., Wei, J., Schuetz, S. et Venkatesh, V. (2021). User compensation as a data breach recovery action: a methodological replication and investigation of generalizability based on the Home Depot breach. *Internet Research*, *31*(3), 765-781. https://doi.org/10.1108/INTR-02-2020-0105

Holling, C. S. (1973). Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics*, *4*, 1-23. https://www.zoology.ubc.ca/bdg/pdfs_bdg/2013/Holling%201973.pdf

Holt, T. J. et Lampke, E. (2010). Exploring stolen data markets online: products and market forces. *Criminal Justice Studies*, *23*(1), 33-50. 10.1080/14786011003634415

Hopkins, M. (2016). Business, victimisation and victimology: reflections on contemporary patterns of commercial victimisation and the concept of businesses as 'ideal victims'. *International Review of Victimology*, *22*(2), 161-178. 10.1177/0269758016628948

Ingram, J. R. et Hinduja, S. (2008). Neutralizing music piracy: an empirical examination. *Deviant Behavior*, *29*(4), 334-366. 10.1080/01639620701588131

Institute for Digital Research and Education. (2021). *One-way MANOVA | Stata data analysis examples*. Institute for Digital Research and Education. https://stats.idre.ucla.edu/stata/dae/one-way-manova/

Ismagilova, E., Slade, E. L., Rana, N. P. et Dwivedi, Y. K. (2019). The effect of electronic word of mouth communications on intention to buy: a meta-analysis. *Information Systems Frontiers*, *22*(5), 1203-1226. 10.1007/s10796-019-09924-y

ISO. (2020). *ISO/IEC 27035-3:2020 information technology — Information security incident management — Part 3: guidelines for ICT incident response operations*. International Organization for Standardization. https://www.iso.org/standard/74033.html

Jackson, S., Vanteeva, N. et Fearon, C. (2019). An investigation of the impact of data breach severity on the readability of mandatory data breach notification letters: evidence from U.S. firms. *Journal of the Association for Information Science and Technology*, *70*(11), 1277-1289. 10.1002/asi.24188

Janoff-Bulman, R., Timko, C. et Carli, L. L. (1985). Cognitive biases in blaming the victim. *Journal of Experimental Social Psychology*, *21*(2), 161-177. 10.1016/0022-1031(85)90013-7

Jansen, J. et Leukfeldt, E. R. (2018). Coping with cybercrime victimization: An exploratory study into impact and change. *Journal of Qualitative Criminal Justice & Criminology*, *2*(2), 205-228. https://www.jqcjc.org/documents/v6i2.pdf#page=78

Jenkins, A., Anandarajan, M. et D'Ovidio, R. (2014). 'All that glitters is not gold': the role of impression management in data breach notification. *Western Journal of Communication*, *78*(3), 337-357. 10.1080/10570314.2013.866686

Jeong, C. Y., Lee, S.-Y. T. et Lim, J.-H. (2019). Information security breaches and IT security investments: impacts on competitors. *Information & Management*, *56*(5), 681-695. https://doi.org/10.1016/j.im.2018.11.003

Johnston, V., Leitner, M., Shapland, J. et Wiles, P. (1994). *Crime on industrial estates*. Home Office Police Research Group. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.561.9477&rep=rep1&type=pdf

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A. et Stulz, R. M. (2020). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, *139*(3), 1-31. 10.1016/j.jfineco.2019.05.019

KeeperSecurity. (2020). *How much is your information worth to a cybercriminal via the Dark Web?* Keeper® Password Manager & Digital Vault. https://keepersecurity.com/how-much-is-my-information-worth-to-hacker-dark-web.html

Kent, C., Tanner, M. et Kabanda, S. (2016). *How South African SMEs address cyber security: The case of web server logs and intrusion detection*. 2016 IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies, Maurice. https://doi.org/10.1109/EmergiTech.2016.7737319

Kim, J. (2019). Underlying processes of SCCT: mediating roles of preventability, blame, and trust. *Public Relations Review*, *45*(3), 1-8. 10.1016/j.pubrev.2019.04.008

Knight, R. et Nurse, J. R. C. (2020). A framework for effective corporate communication after cyber security incidents. *Computers & Security*, *99*, 1-18. https://doi.org/10.1016/j.cose.2020.102036

Ko, M. et Dorantes, C. (2006). The impact of information security breaches on financial performance of the breached firms: an empirical investigation. *Journal of Information Technology Management*, *17*(2), 13-22. https://jitm.ubalt.edu/XVII-2/article2.pdf

Kont, M., Pihelgas, M., Wojtkowiak, J., Trinberg, L. et Osula, A.-M. (2018). *Insider threat detection study*. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2018/10/Insider_Threat_Study_CCDCOE.pdf

Lasky, N. V. (2019). Victim precipitation theory. Dans F. P. Bernat, K. Frailing, L. Gelsthorpe, S. Kethineni et L. Pasko (eds.), *The Encyclopedia of women and crime* (p. 1-2). 10.1002/9781118929803.ewac0517

LastPass. (2020). *Psychology of passwords: The online behavior that's putting you at risk*. LastPass. https://lp-cdn.lastpass.com/lporcamedia/document-library/lastpass/pdf/en/LastPass-B2C-Assets-Ebook.pdf

Laube, S. et Böhme, R. (2016). The economics of mandatory security breach reporting to authorities. *Journal of Cybersecurity*, *2*(1), 29-41. 10.1093/cybsec/tyw002

LeBel, S. (2020). Projet de loi no 64 : loi modernisant des dispositions législatives en matière de protection des renseignements personnels. http://www.assnat.qc.ca/Media/Process.aspx?MediaId=ANQ.Vigie.Bll.DocumentGenerique_159567&process=Default&token=ZyMoxNwUn8ikQ+TRKYwPCjWrKwg+vIv9rjij7p3xLGTZDmLVSmJLoqe/vG7/YWzz

Lerner, M. J. et Miller, D. T. (1978). Just World research and the attribution process: looking back and ahead. *Psychological Bulletin*, *85*(5), 1030-1051. https://doi.org/10.1037/0033-2909.85.5.1030

Lewis, J. A., Hamilton, J. C. et Elmore, J. D. (2019). Describing the ideal victim: a linguistic analysis of victim descriptions. *Current Psychology*. 10.1007/s12144-019-00347-1

Libicki, M. C., Ablon, L. et Webb, T. (2015). *The defender's dilemma: charting a course toward cybersecurity*. RAND Corporation. https://www.rand.org/pubs/research_reports/RR1024.html

Lodewijkx, H. F. M., Wildschut, T., Nijstad, B. A., Savenije, W. et Smit, M. (2001). In a violent world a just world makes sense: the Case of "senseless violence" in the Netherlands. *Social Justice Research*, *14*(1), 79-94. https://doi.org/10.1023/A:1012527808620

Lucia, S., Herrmann, L., et Killias, M. (2007). How important are interview methods and questionnaire designs in research on self-reported juvenile delinquency? An experimental comparison of Internet vs paper-and-pencil questionnaires and different

definitions of the reference period. *Journal of Experimental Criminology*, *3*(1), 39-64. https://doi.org/10.1007/s11292-007-9025-1

Lutz-Zois, C. J., Moler, K. A. et Brown, M. J. (2015). Mechanisms for the relationship between traditional masculine ideologies and rape myth acceptance among college men, *Journal of Aggression, Maltreatment & Trauma*, *24*(1), 84-101. 10.1080/10926771.2015.996311

Madarie, R., Ruiter, S., Steenbeek, W. et Kleemans, E. (2019). Stolen account credentials: an empirical comparison of online dissemination on different platforms. *Journal of Crime and Justice*, *42*(5), 551-568. 10.1080/0735648X.2019.1692418

Malhotra, A. et Malhotra, K. C. (2011). Evaluating customer information breaches as service failures: an event study approach. *Journal of Service Research*, *14*(1), 44-59. 10.1177/1094670510383409

Malhotra, N., Sahadev, S. et Purani, K. (2017). Psychological contract violation and customer intention to reuse online retailers: exploring mediating and moderating mechanisms. *Journal of Business Research*, *75*, 17-28. 10.1016/j.jbusres.2017.01.013

Marciniak, L. M. (1998). Adolescent attitudes toward victim precipitation of rape, *Violence and Victims*, *13*(3), 287-300. 10.1891/0886-6708.13.3.287

Martin, K. (2020). Breaking the privacy paradox: the value of privacy and associated duty of firms. *Business Ethics Quarterly*, *30*(1), 65-96. https://doi.org/10.1017/beq.2019.24

Mason, G. (2013). The symbolic purpose of hate crime law: ideal victims and emotion. *Theoretical Criminology*, *18*, 75-92. 10.1177/1362480613499792

Masten, A. S. (2018). Resilience theory and research on children and families: past, present, and promise. *Journal of Family Theory & Review*, *10*(1), 12-31. 10.1111/jftr.12255

Matheu, S. N., Hernández-Ramos, J. L., Skarmeta, A. F. et Baldini, G. (2021). A Survey of Cybersecurity Certification for the Internet of Things. *ACM Computing Surveys*, *53*(6), 1-36. https://doi.org/10.1145/3410160

Maynes, M. (2019). *One simple action you can take to prevent 99.9 percent of attacks on your accounts*. Microsoft Security. https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/

McGurrin, D., Jarrell, M., Jahn, A. et Cochrane, B. (2013). White collar crime representation in the criminological literature revisited, 2001-2010. *Journal of the Western Society of Criminology*, *14*(2), 3-19. https://www.academia.edu/19256618/White_Collar_Crime_Representation_in_the_Criminological_Literature_Revisited_2001-2010

Miethe, T. D. (1985). The myth or reality of victim involvement in crime: a review and comment on victim-precipitation research. *Sociological Focus*, *18*(3), 209-220. https://www.jstor.org/stable/20831364

Miller, J. C. et Angelis, J. N. (2018). *An empirical investigation of the effects of individuality on responses to data theft crimes*. 2018 IEEE Technology and Engineering Management Conference, Evanston, IL, États-Unis. 10.1109/TEMSCON.2018.8488430

Mirian, A., DeBlasio, J., Savage, S., Voelker, G. M. et Thomas, K. (2019). *Hack for hire: exploring the emerging market for account hijacking*. WWW '19: The World Wide Web Conference, San Francisco, CA, États-Unis. 10.1145/3308558.3313489

Moreau, G. (2021). *Statistiques sur les crimes déclarés par la police au Canada, 2020*. Statistique Canada. https://www150.statcan.gc.ca/n1/pub/85-002-x/2021001/article/00013-fra.htm#a17

Morreale, T. (2008). *Incident handling for SMEs (small to medium enterprises)*. SANS Institute. https://www.sans.org/reading-room/whitepapers/incident/incident-handling-smes-small-medium-enterprises-32764

Morrison, K. E., Luchok, K. J., Richter, D. L. et Parra-Medina, D. (2006). Factors influencing help-seeking from informal networks among African American victims of intimate partner violence. *Journal of Interpersonal Violence*, *21*(11), 1493-1511. 10.1177/0886260506293484

Morse, E., Raval, V. et Wingender, J. (2011). Market price effects of data security breaches. *Information Security Journal: A Global Perspective*, *20*, 263-273. 10.1080/19393555.2011.611860

Multivariate Analysis of Variance. s.d. Multivariate Analysis of Variance. https://www.sagepub.com/sites/default/files/upm-assets/9761_book_item_9761.pdf

Muzatko, S. et Bansal, G. (2018). *Timing of data breach announcement and e-commerce trust*. Midwest Association for Information 2018 Proceedings, Saint-Louis, Missouri, États-Unis. https://aisel.aisnet.org/mwais2018/7/?utm_source=aisel.aisnet.org%2Fmwais2018%2F7&utm_medium=PDF&utm_campaign=PDFCoverPages

NCSC. (2020). *Response and recovery - Small business guide: how to prepare your response to (and plan your recovery from) a cyber incident*. National Cyber Security Centre. https://www.ncsc.gov.uk/files/NCSC_A5%20Response%20and%20Recovery%20Guide_v3_OCT20.pdf

Ng, Z. X., Ahmad, A. et Maynard, S. B. (2013). *Information security management: factors that influence security investments in SMES*. 11th Australian Information Security Management Conference, Perth, Australie. http://ro.ecu.edu.au/ism/157

Nieuwesteeg, B. et Faure, M. (2018). An analysis of the effectiveness of the EU data breach notification obligation. *Computer Law & Security Review*, *34*(6), 1232-1246. 10.1016/j.clsr.2018.05.026

NIST. (2015). Disaster resilience framework—Glossary. National Institute of Standards and Technology. https://www.nist.gov/system/files/documents/el/building_materials/resilience/Glossary_75-_11Feb2015-2.pdf

NIST. (2018). *Framework for improving critical infrastructure cybersecurity, version 1.1*. National Institute of Standards and Technology. 10.6028/NIST.CSWP.04162018

Novak, A. N. et Vilceanu, M. O. (2019). "The internet is not pleased": Twitter and the 2017 Equifax data breach. *The Communication Review*, *22*(3), 196-221. 10.1080/10714421.2019.1651595

OED Online. (2020). *resilience, n.* Oxford University Press. https://www.oed.com/view/Entry/163619

Ohm, P. (2008). The myth of the superuser: fear, risk, and harm online. *UC Davis Law Review*, *41*(4), 1327-1402. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=967372

Peretti, K. (2009). Data breaches: what the underground world of carding reveals. *Santa Clara High Technology Law Journal*, *25*(2), 375-414. https://digitalcommons.law.scu.edu/chtlj/vol25/iss2/4

Peterson, R. A. (2001). On the Use of College Students in Social Science Research: Insights from a Second-Order Meta-analysis. *Journal of Consumer Research*, *28*(3), 450-461. https://doi.org/10.1086/323732

Ping Identity. (2019). *2019 consumer survey: trust and accountability in the era of data misuse*. Ping Identity. https://www.pingidentity.com/content/dam/ping-6-2-assets/Assets/Misc/en/3464-consumersurvey-execsummary.pdf

Piquero, N. L., Cohen, M. A. et Piquero, A. R. (2011). How much is the public willing to pay to be protected from identity theft? *Justice Quarterly*, *28*(3), 437-459. 10.1080/07418825.2010.511245

Ponemon. (2014). *The aftermath of a data breach: consumer sentiment*. Ponemon Institute. https://www.ponemon.org/local/upload/file/Consumer%20Study%20on%20Aftermath%20of%20a%20Breach%20FINAL%202.pdf

Ponemon. (2017). *The impact of data breaches on reputation & share value*. Ponemon Institute. https://www.centrify.com/media/4772757/ponemon_data_breach_impact_study_uk.pdf

Ponemon. (2019). *2019 cost of a data breach report*. Ponemon Institute. https://www.all-about-security.de/fileadmin/micropages/Fachartikel_28/2019_Cost_of_a_Data_Breach_Report_final.pdf

Privacy Rights Clearinghouse. (2019). *What to do when you receive a data breach notice*. Privacy Rights Clearinghouse. https://privacyrights.org/consumer-guides/what-do-when-you-receive-data-breach-notice

Proofpoint. (2020). *2020 State of the Phish: an in-depth look at user awareness, vulnerability and resilience*. Proofpoint. https://cdw-prod.adobecqms.net/content/dam/cdw/on-domain-cdw/brands/proofpoint/gtd-pfpt-us-tr-state-of-the-phish-2020.pdf

Reurink, A. (2016). “White-collar crime”: The concept and its potential for the analysis of financial crime. *European Journal of Sociology / Archives Européennes de Sociologie*, *57*(3), 385-415. 10.1017/S0003975616000163

Reyns, B. W. et Henson, B. (2016). The thief with a thousand faces and the victim with none: identifying determinants for online identity theft victimization with routine activity theory. *International Journal of Offender Therapy and Comparative Criminology*, *60*(10), 1119-1139. 10.1177/0306624X15572861

Richardson, R. (2011). *2010/2011 computer crime and security survey*. Computer Security Institute. https://cours.etsmtl.ca/gti619/documents/divers/CSIsurvey2010.pdf

Rieb, A., Gurschler, T. et Lechner, U. (2017). A gamified approach to explore techniques of neutralization of threat actors in cybercrime. Dans E. Schweighofer, H. Leitold, A. Mitrakas et K. Rannenberg (dir.), *Privacy technologies and policy* (p. 87-103). Springer. 10.1007/978-3-319-67280-9_5

RiskBased Security (2020). *2020 mid year report*: *data breach quickview*. https://pages.riskbasedsecurity.com/hubfs/Reports/2020/2020%20Mid%20Year%20Data%20Breach%20QuickView%20Report.pdf

Romanosky, S., Hoffman, D. et Acquisti, A. (2014). Empirical analysis of data breach litigation. *Journal of Empirical Legal Studies*, *11*(1), 74-104. 10.1111/jels.12035

Romanosky, S., Telang, R. et Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis and Management*, *30*(2), 256-286. 10.1002/pam.20567

Rosati, P., Deeney, P., Cummins, M., van der Werff, L. et Lynn, T. (2019). Social media and stock price reaction to data breach announcements: evidence from US listed companies. *Research in International Business and Finance*, *47*, 458-469. 10.1016/j.ribaf.2018.09.007

Sable, M. R., Danis, F., Mauzy, D. L. et Gallagher, S. K. (2006). Barriers to reporting sexual assault for women and men: perspectives of college students. *Journal of American College Health*, *55*(3), 157-162. 10.3200/JACH.55.3.157-162

Salesforce. (2018). *State of the connected customer*. Salesforce. https://www.salesforce.com/content/dam/web/en_us/www/documents/e-books/state-of-the-connected-customer-report-second-edition2018.pdf

Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K.-K. R. et Burnap, P. (2020). Impact and key challenges of insider threats on organizations and critical businesses. *Electronics*, *9*(9), 1-29. https://doi.org/10.3390/electronics9091460

Schatz, D. et Bashroush, R. (2016). The impact of repeated data breach events on organisations' market value. *Information & Computer Security*, *24*(1), 73-92. 10.1108/ICS-03-2014-0020

Schneider, H. (2014). The corporation as victim of white collar crime: results from a study of German public and private companies. *University of Miami International and Comparative Law Review*, *22*, 171-205. https://repository.law.miami.edu/cgi/viewcontent.cgi?article=1274&context=umiclr

Schwab, K. (2016). *The Fourth Industrial Revolution: what it means, how to respond*. World Economic Forum. https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

Schwarz, J., Gibson, S. et Lewis-Arévalo, C. (2017). Sexual assault on college campuses: substance use, victim status awareness, and barriers to reporting. *Building Healthy Academic Communities Journal*, *1*(2), 45-60. 10.18061/bhac.v1i2.5520

Shay, R., Ion, I., Reeder, R. W. et Consolvo, S. (2014). *« My religious aunt asked why i was trying to sell her Viagra »: experiences with account hijacking*. Proceedings of Conference on Human Factors in Computing Systems 2014, Toronto, ON, Canada. 10.1145/2556288.2557330

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J. et Nunge, E. (2007). *Anti-Phishing Phil: the design and evaluation of a game that teaches people not to fall for phish*. Proceedings of the 3rd Symposium on Usable Privacy and Security, Pittsburgh, Pennsylvanie, États-Unis. 10.1145/1280680.1280692

Sjouwerman, S. (2017). *Phishing and social engineering in 2018: is the worst yet to come?* KnowBe4. https://www.knowbe4.com/hubfs/PhishingandSocialEngineeringin2018.pdf

Stack, B. (2017). *Here's how much your personal information is selling for on the dark web*. Experian. https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/

Statistics Canada. (2018). *Canadian survey of cyber security and cybercrime*. Statistics Canada. https://www.serene-risc.ca/en/statistics-canada

Statistique Canada. (2020). *Enquête canadienne sur la cybersécurité et le cybercrime (ECCC)*. Statistique Canada. https://www.statcan.gc.ca/fra/enquete/entreprise/5244

Steel, C. (2019). Stolen identity valuation and market evolution on the dark web. *International Journal of Cyber Criminology*, *13*(1). 10.5281/zenodo.3539500

Stockman, M., Nedelec, J. et Mackey, W. (2017). Organizational cybervictimization: data breach prevention using a victimological approach. Dans T. J. Holt (eds.), *Cybercrime through an interdisciplinary lens* (p. 127-149). Routledge. https://www.taylorfrancis.com/books/e/9781315618456

Strömwall, L. A., Alfredsson, H. et Landström, S. (2013). Rape victim and perpetrator blame and the Just World hypothesis: The influence of victim gender and age. *Journal of Sexual Aggression*, *19*(2), 207-217. https://doi.org/10.1080/13552600.2012.683455

Sullivan, R. J. et Maniff, J. L. (2016). Data breach notification laws. *Economic Review*, *101*(1), 65-85. https://econpapers.repec.org/article/fipfedker/00037.htm

Sutherland, E. H. (1940). White-collar criminality. *American Sociological Review*, *5*(1), 1-12. 10.2307/2083937

Swinhoe, D. (2020*). The 15 biggest data breaches of the 21st century*. CSO Online. https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

Syed, R. (2019). Enterprise reputation threats on social media: a case of data breach framing. *The Journal of Strategic Information Systems*, *28*(3), 257-274. 10.1016/j.jsis.2018.12.001

Syed, R. et Dhillon, G. (2015). *Dynamics of data breaches in online social networks: understanding threats to organizational information security reputation*. Thirty Sixth International Conference on Information Systems, Fort Worth, TX, États-Unis. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1676&context=icis2015

Sykes, G. M. et Matza, D. (1957). Techniques of neutralization: a theory of delinquency. *American Sociological Review*, *22*(6), 664-670. 10.2307/2089195

Symantec. (2014). *The cyber resilience blueprint: a new perspective on security*. Symantec. https://www.symantec.com/content/en/us/enterprise/white_papers/b-cyber-resilience-blueprint-wp-0814.pdf

The Economist Intelligence Unit. (2016). *Protecting the brand - cyber-attacks and the reputation of the enterprise*. The Economist. https://eiuperspectives.economist.com/sites/default/files/images/EIU-VMware%20Protectingthebrand_PDF.pdf

Timmer, D. A. et Norman, W. H. (1984). The ideology of victim precipitation. *Criminal Justice Review*, *9*(2), 63-68. 10.1177/073401688400900209

Trend Micro. (2017). *What do Hackers do with Your Stolen Identity? - Security News - Trend Micro USA*. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/what-do-hackers-do-with-your-stolen-identity

Tweneboah-Kodua, S., Atsu, F. et Buchanan, W. (2018). Impact of cyberattacks on stock performance: a comparative study. *Information & Computer Security*, *26*(5), 637-652. 10.1108/ICS-05-2018-0060

Tweneboah-Koduah, S., Atsu, F. et Prasad, R. (2020). Reaction of stock volatility to data breach: an event study. *Journal of Cyber Security and Mobility*, *9*(3), 1-19. 10.13052/jcsm2245-1439.931

Valecha, R., Bachura, E., Chen, R. et Raghav Rao, H. (2017). An exploration of public reaction to the OPM data breach notifications. Dans M. Fan, J. Heikkilä, H. Li, M. J. Shaw et H. Zhang (dir.), *Internetworked World* (p. 185-191). Springer. 10.1007/978-3-319-69644-7_19

van den Bos, K. et Maas, M. (2009). On the psychology of the belief in a just world: exploring experiential and rationalistic paths to victim blaming. *Personality and Social Psychology Bulletin*, *35*(12), 1567-1578. https://doi.org/10.1177/0146167209344628

van der Bruggen, M. et Grubb, A. (2014). A review of the literature relating to rape victim blaming: An analysis of the impact of observer and victim characteristics on attribution of blame in rape cases. *Aggression and Violent Behavior*, *19*(5), 523-531. 10.1016/j.avb.2014.07.008

van Wijk, J. (2013). Who is the 'little old lady' of international crimes? Nils Christie's concept of the ideal victim reinterpreted. *International Review of Victimology*, *19*(2), 159-179. https://doi.org/10.1177/0143034312472770

Vassakis, K., Petrakis, E. et Kopanakis, I. (2018). Big Data Analytics: Applications, Prospects and Challenges. Dans G. Skourletopoulos, G. Mastorakis, C. X. Mavromoustakis, C. Dobre et E. Pallis (dir.), *Mobile big data: a roadmap from models to technologies* (p. 3-20). Springer International Publishing. 10.1007/978-3-319-67925-9_1

Verhagen, T., Nauta, A. et Feldberg, F. (2013). Negative online word-of-mouth: behavioral indicator or emotional release?. *Computers in Human Behavior*, *29*(4), 1430-1440. 10.1016/j.chb.2013.01.043

Verizon. (2021). *2021 data breach investigations report*. Verizon. https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2021-data-breach-investigations-report.pdf

von Tigerstrom, B. (2018). Direct and vicarious liability for tort claims involving violation of privacy. *The Canadian Bar Review*, *96*(3), 539-564. https://cbr.cba.org/index.php/cbr/article/view/4483

Vonderhaar, R. L. et Carmody, D. C. (2015). There are no "innocent victims": the influence of Just World beliefs and prior victimization on rape myth acceptance. *Journal of Interpersonal Violence*, *30*(10), 1615-1632. https://doi.org/10.1177/0886260514549196

Wall, D. S. (2008). Cybercrime and the culture of fear. *Information, Communication & Society*, *11*(6), 861-884. 10.1080/13691180802007788

Wang, P. et Park, S.-A. (2017). Communication in cybersecurity: a public communication model for business data breach incident handling. *Issues in Information Systems*, *18*(2), 136-147. http://www.iacis.org/iis/2017/2_iis_2017_136-147.pdf

Wartick, S. L. (1992). The relationship between intense media exposure and change in corporate reputation. *Business & Society*, *31*(1), 33-49. 10.1177/000765039203100104

Wemmers, J. (2017). *Victimologie : une perspective canadienne*. Presses de l'Université du Québec.

Wen, Z. A., Lin, Z., Chen, R. et Andersen, E. (2019). *What.Hack: engaging anti-phishing training through a role-playing phishing simulation game*. Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, Glasgow, Écosse, Royaume-Uni. 10.1145/3290605.3300338

Werner, E. E. (1995). Resilience in development. *Current Directions in Psychological Science*, *4*(3), 81-85. https://www.jstor.org/stable/20182335

West, B. (2016). Chapter 7 – Communicating before, during and after a breach. Dans K. Fowler (dir.), *Data breach preparation and response: breaches are certain, impact is not* (p. 167-185). Syngress. 10.1016/B978-0-12-803451-4.00007-1

Whitson, J. R. et Haggerty, K. D. (2008). Identity theft and the care of the virtual self. *Economy and Society*, *37*(4), 572-594. 10.1080/03085140802357950

Wolfgang, M. F. (1957). Victim precipitated criminal homicide. *The Journal of Criminal Law, Criminology, and Police Science*, *48*(1), 1-11. https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=4565&context=jclc

Ylang, N. (2020). Capable guardianship against identity theft: demographic insights based on a national sample of US adults. *Journal of Financial Crime*, *27*(1), 130-142. 10.1108/JFC-12-2018-0140

Zaiss, J., Zaeem, R. N. et Barber, K. S. (2019). Identity threat assessment and prediction. *Journal of Consumer Affairs*, *53*(1), 58-70. 10.1111/joca.12191

Zaykowski, H., Kleinstuber, R. et McDonough, C. (2014). Judicial narratives of ideal and deviant victims in judges' capital sentencing decisions. *American Journal of Criminal Justice*, *39*(4), 716-731. https://doi.org/10.1007/s12103-014-9257-3

Zou, Y. et Schaub, F. (2019). Beyond mandatory: making data breach notifications useful for consumers. *IEEE Security & Privacy*, *17*(2), 67-72. 10.1109/MSEC.2019.2897834

Zou, Y., Mhaidli, A. H., McCall, A. et Schaub, F. (2018). *« I've got nothing to lose »: consumers' risk perceptions and protective actions after the Equifax data breach*. Fourteenth Symposium on Usable Privacy and Security, Baltimore, MD, États-Unis. https://www.usenix.org/conference/soups2018/presentation/zou

ANNEXE 1

Vignette de cas 1

Boîte à prix est une petite entreprise canadienne spécialisée dans la vente au détail. Elle a subi un vol de données ayant touché les noms et adresses courriel d'un nombre limité de clients. Après avoir détecté la brèche, la firme a immédiatement lancé un avis public par lequel elle a affirmé qu'elle avait en place une gamme complète de procédés et des technologies pour prévenir les incidents de sécurité, et qu'elle a des mesures pour empêcher le mésusage des données dans l'éventualité qu'une fuite survienne. Regrettant l'incident, Boîte à prix a été très communicative sur les circonstances de la brèche ainsi que sur les façons de se protéger de la fraude à l'identité, et a laissé ouvertes ses chaînes de communications, au cas où les clients auraient des questions.

Vignette de cas 2

Boîte à prix est une petite entreprise canadienne spécialisée dans la vente au détail. Elle a subi un vol de données ayant touché les noms et adresses courriel d'un nombre limité de clients. Après avoir détecté la fuite, le commerce a attendu deux mois avant de lancer un avis public désinvolte. Boîte à prix est réticente de partager ses pratiques de sécurité, mais la couverture médiatique suggère que sa culture de cybersécurité est lacunaire et qu'elle n'a pas de mesures en place pour prévenir le mésusage des données volées. Enfin, la firme a été peu communicative sur les circonstances de la brèche ainsi que sur les façons de se protéger de la fraude à l'identité, et a gardé fermées ses chaînes de communications, empêchant ainsi les clients de poser des questions.

Vignette de cas 3

ÉchangeGros est une grande entreprise canadienne spécialisée dans la vente au détail. Elle a subi un vol de données ayant touché les noms et adresses courriel d'un nombre limité de clients. Après avoir détecté la brèche, la firme a immédiatement lancé un avis public par lequel elle a affirmé qu'elle avait en place une gamme complète de procédés et des technologies pour prévenir les incidents de sécurité, et qu'elle a des mesures pour empêcher le mésusage des données dans l'éventualité qu'une fuite survienne. Regrettant l'incident, ÉchangeGros a été très communicative sur les circonstances de la brèche ainsi que sur les façons de se protéger de la fraude à l'identité, et a laissé ouvertes ses chaînes de communications, au cas où les clients auraient des questions.

Vignette de cas 4

ÉchangeGros est une grande entreprise canadienne spécialisée dans la vente au détail. Elle a subi un vol de données ayant touché les noms et adresses courriel d'un nombre limité de clients. Après avoir détecté la fuite, le commerce a attendu deux mois avant de lancer un avis public désinvolte. ÉchangeGros est réticente de partager ses pratiques de sécurité, mais la couverture médiatique suggère que sa culture de cybersécurité est lacunaire et qu'elle n'a pas de mesures en place pour prévenir le mésusage des données volées. Enfin, la firme a été peu communicative sur les circonstances de la brèche ainsi que sur les façons de se protéger de la fraude à l'identité, et a gardé fermées ses chaînes de communications, empêchant ainsi les clients de poser des questions.

Vignette de cas 5

Boîte à prix est une petite entreprise canadienne spécialisée dans la vente au détail. Elle a subi un vol de données ayant touché les informations de cartes de crédit d'un grand nombre de ses clients. Après avoir détecté la brèche, la firme a immédiatement lancé un avis public par lequel elle a affirmé qu'elle avait en place une gamme complète de procédés et des technologies pour prévenir les incidents de sécurité, et qu'elle a des mesures pour empêcher le mésusage des données dans l'éventualité qu'une fuite survienne. Regrettant l'incident, Boîte à prix a été très communicative sur les circonstances de la brèche ainsi que sur les façons de se protéger de la fraude à l'identité, et a laissé ouvertes ses chaînes de communications, au cas où les clients auraient des questions.

Vignette de cas 6

Boîte à prix est une petite entreprise canadienne spécialisée dans la vente au détail. Elle a été la victime d'un vol de données ayant touché les informations de cartes de crédit d'un grand nombre de ses clients. Après avoir détecté la fuite, le commerce a attendu deux mois avant de lancer un avis public désinvolte. Boîte à prix est réticente de partager ses pratiques de sécurité, mais la couverture médiatique suggère que sa culture de cybersécurité est lacunaire et qu'elle n'a pas de mesures en place pour prévenir le mésusage des données volées. Enfin, la firme a été peu communicative sur les circonstances de la brèche ainsi que sur les façons de se protéger de la fraude à l'identité, et a gardé fermées ses chaînes de communications, empêchant ainsi les clients de poser des questions.

Vignette de cas 7

ÉchangeGros est une grande entreprise canadienne spécialisée dans la vente au détail. Elle a subi un vol de données ayant touché les informations de cartes de crédit d'un grand nombre de ses clients. Après avoir détecté la brèche, la firme a immédiatement lancé un avis public par lequel elle a affirmé qu'elle avait en place une gamme complète de procédés et des technologies pour prévenir les incidents de sécurité, et qu'elle a des mesures pour empêcher le mésusage des données dans l'éventualité qu'une fuite survienne. Regrettant l'incident, ÉchangeGros a été très communicative sur les circonstances de la brèche ainsi que sur les façons de se protéger de la fraude à l'identité, et a laissé ouvertes ses chaînes de communications, au cas où les clients auraient des questions.

Vignette de cas 8

ÉchangeGros est une grande entreprise canadienne spécialisée dans la vente au détail. Elle a été la victime d'un vol de données ayant touché les informations de cartes de crédit d'un grand nombre de ses clients. Après avoir détecté la fuite, le commerce a attendu deux mois avant de lancer un avis public désinvolte. ÉchangeGros est réticente de partager ses pratiques de sécurité, mais la couverture médiatique suggère que sa culture de cybersécurité est lacunaire et qu'elle n'a pas de mesures en place pour prévenir le mésusage des données volées. Enfin, la firme a été peu communicative sur les circonstances de la brèche ainsi que sur les façons de se protéger de la fraude à l'identité, et a gardé fermées ses chaînes de communications, empêchant ainsi les clients de poser des questions.

ANNEXE 2

Imaginez que vous êtes client(e) de l'entreprise dans la mise en situation…

	Tout à fait d'accord	D'accord	Plutôt d'accord	Indifférent	Plutôt pas d'accord	Pas d'accord	Pas du tout d'accord
Je pense que le vol de données est la faute de l'entreprise.							
J'éprouve des sentiments négatifs à l'égard de l'entreprise.							
Je pense que l'entreprise peut adéquatement surmonter ce nouveau défi.							
Je dirais des commentaires positifs à propos de l'entreprise à mon entourage.							
Je continuerais de fréquenter l'entreprise.							
J'intenterais un recours collectif contre l'entreprise si j'en avais le pouvoir.							

1. Quel est votre genre ? (Choisissez une réponse)

□ Homme

□ Femme

□ Autre

2. Quel est votre âge ?

_____

3. Quel diplôme détenez-vous en ce moment ? (Choisissez une réponse)

□ Aucun diplôme

□ Diplôme secondaire

□ Diplôme collégial

□ Diplôme baccalauréat

□ Diplôme de maîtrise

□ Diplôme de doctorat

□ Autre

4. Quelle est votre origine ethnique ? (Choisissez une réponse)

□ Peuples autochtones

□ Asiatique

□ Noire

□ Blanche

□ Hispanique

□ Autre

5. À quelle université êtes-vous inscrit en ce moment ?

_____

6. Quel est votre programme d'étude actuel ?

_____

7. Inscrivez votre adresse courriel si vous souhaitez recevoir les résultats principaux à la fin de la recherche.

_____

ANNEXE 3

Université de Montréal

Comité d'éthique de la recherche – Société et culture (CER-SC)

26 novembre 2020

Objet: Approbation éthique – L'impact de la cyber-résilience sur la réaction du public à la suite d'une brèche de données chez les entreprises canadiennes

M. Traian Toma,

Le Comité d'éthique de la recherche – société culture (CERSC) de l'Université de Montréal a étudié le projet de recherche susmentionné et a délivré le certificat d'éthique demandé suite à la satisfaction des exigences précédemment émises. Vous trouverez ci-joint une copie numérisée de votre certificat. Nous vous invitons à faire suivre ce document au technicien en gestion de dossiers étudiants (TGDE) de votre département.

Notez qu'il y apparaît une mention relative à un suivi annuel et que le certificat comporte une date de fin de validité. En effet, afin de répondre aux exigences éthiques en vigueur au Canada et à l'Université de Montréal, nous devons exercer un suivi annuel auprès des chercheurs et étudiants-chercheurs.

De manière à rendre ce processus le plus simple possible, nous avons élaboré un court questionnaire qui vous permettra à la fois de satisfaire aux exigences du suivi et de nous faire part de vos commentaires et de vos besoins en matière d'éthique en cours de recherche. Ce questionnaire de suivi devra être rempli annuellement jusqu'à la fin du projet et pourra nous être retourné par courriel. La validité de l'approbation éthique est conditionnelle à ce suivi. Sur réception du dernier rapport de suivi en fin de projet, votre dossier sera clos.

Il est entendu que cela ne modifie en rien l'obligation pour le chercheur, tel qu'indiqué sur le certificat d'éthique, de signaler au CERSC tout incident grave dès qu'il survient ou de lui faire part de tout changement anticipé au protocole de recherche.

Nous vous prions d'agréer l'expression de nos sentiments les meilleurs.

[redacted]

Anne Marie Tassé, présidente
Comité d'éthique de la recherche – Société et culture (CER-SC)
Université de Montréal

c. c. David Décary-Hétu, professeur agrégé, FAS - École de criminologie
Benoît Dupont, Professeur titulaire , FAS - École de criminologie

p. j. Certificat #CERSC-2020-123-D

adresse postale
C.P. 6128, succ. Centre-ville
Montréal QC H3C 3J7

adresse civique
3333, Queen Mary
Local 220
Montréal QC H3V 1A2

Téléphone : 514-343-7338
cersc@umontreal.ca
cersc.umontreal.ca

Université de Montréal

Nº de certificat
CERSC-2020-123-D

Comité d'éthique de la recherche – Société et culture (CER-SC)

CERTIFICAT D'APPROBATION ÉTHIQUE

Le Comité d'éthique de la recherche – société et culture (CER-SC) selon les procédures en vigueur, en vertu des documents qui lui ont été fournis, a examiné le projet de recherche suivant et conclu qu'il respecte les règles d'éthique énoncées dans la Politique sur la recherche avec des êtres humains de l'Université de Montréal.

Projet	
Titre du projet	**L'impact de la cyber-résilience sur la réaction du public à la suite d'une brèche de données chez les entreprises canadiennes**
Requérant	**Traian Toma**, candidat à la maîtrise, FAS – École de criminologie
Sous la direction de:	David Décary-Hétu, professeur agrégé, FAS - École de criminologie, Université de Montréal & Benoît Dupont, Professeur titulaire , FAS - École de criminologie, Université de Montréal.

Financement	
Organisme	Non financé

MODALITÉS D'APPLICATION

Tout changement anticipé au protocole de recherche doit être communiqué au Comité qui en évaluera l'impact au chapitre de l'éthique. Toute interruption prématurée du projet ou tout incident grave doit être immédiatement signalé au Comité. Selon les règles universitaires en vigueur, un suivi annuel est minimalement exigé pour maintenir la validité de la présente approbation éthique, et ce, jusqu'à la fin du projet. Le questionnaire de suivi est disponible sur la page web du Comité.

[redacted]

Anne-Marie Tassé, présidente
Comité d'éthique de la recherche – Société et culture (CER-SC)
Université de Montréal

26 novembre 2020
Date de délivrance

1 décembre 2021
Date de fin de validité

1 décembre 2021
Date du prochain suivi

3537

UQTR
Savoir.
Surprendre.

CERTIFICAT D'ÉTHIQUE DE LA RECHERCHE AVEC DES ÊTRES HUMAINS

En vertu du mandat qui lui a été confié par l'Université, le Comité d'éthique de la recherche avec des êtres humains a analysé et approuvé pour certification éthique le protocole de recherche suivant :

Titre : **L'impact de la cyber-résilience sur la réaction du public à la suite d'une brèche de données chez les entreprises canadiennes**

Chercheur(s) : Traian Toma
École de criminologie

Organisme(s) : Aucun financement

N° DU CERTIFICAT : **CER-20-272-11.02**

PÉRIODE DE VALIDITÉ : **Du 01 décembre 2020 au 01 décembre 2021**

En acceptant le certificat éthique, le chercheur s'engage à :

- Aviser le CER par écrit des changements apportés à son protocole de recherche avant leur entrée en vigueur;
- Procéder au renouvellement annuel du certificat tant et aussi longtemps que la recherche ne sera pas terminée;
- Aviser par écrit le CER de l'abandon ou de l'interruption prématurée de la recherche;
- Faire parvenir par écrit au CER un rapport final dans le mois suivant la fin de la recherche.

[redacted]

Me Richard LeBlanc
Président du comité

[redacted]

Fanny Longpré
Secrétaire du comité

Décanat de la recherche et de la création

Date d'émission : 01 décembre 2020

UNIVERSITÉ LAVAL

Vice-rectorat à la recherche et à la création
Comité d'éthique de la recherche

APPROBATION DE L'ÉTHIQUE

Projet de recherche impliquant des êtres humains ou la consultation de renseignements personnels

Ce projet de recherche a été examiné en conformité avec les *Modalités de gestion de l'éthique de la recherche sur des êtres humains* de l'Université Laval, par le Comité plurifacultaire d'éthique de la recherche

Projet intitulé :	**L'impact de la cyber-résilience sur la réaction du public à la suite d'une brèche de données chez les entreprises canadiennes**
Nom du chercheur :	**Monsieur Traian Toma**
Nom du directeur de recherche :	**Monsieur David Décary-Hétu**
Numéro d'approbation :	**2020-398 / 18-012021**
Date de décision :	**18 janvier 2021**
Date d'expiration de l'approbation :	**1er février 2022**

Après examen des informations et des documents qui lui ont été transmis, le Comité a constaté que ce projet respecte les principes d'éthique de la recherche avec des êtres humains. Il prend acte de la confirmation écrite du chercheur à l'effet qu'il a pris connaissance des mesures de suivi[1] associées à l'émission de l'approbation éthique de son projet et qu'il accepte de les appliquer. « Par conséquent, le Comité approuve ce projet pour un an ».

[redacted]

Sabrina Doyon, coprésidente
Comité plurifacultaire d'éthique de la recherche

20 janvier 2021
Date

[1] Rappel des mesures de suivi au verso

Maison Michael-John-Brophy
2241, chemin Sainte-Foy
Québec (Québec) G1V 0A6
CANADA

418 656-2131, poste 4606
Télécopieur : 418 656-2040
cer@vrr.ulaval.ca
www.vrr.ulaval.ca

UNIVERSITÉ LAVAL

Vice-rectorat à la recherche et à la création
Comité d'éthique de la recherche

Mesures de suivi associées à l'approbation éthique

Pour le projet intitulé : « L'impact de la cyber-résilience sur la réaction du public à la suite d'une brèche de données chez les entreprises canadiennes »

Numéro de dossier : 2020-398

1. Informer le Comité par écrit et dans les meilleurs délais (indépendamment du calendrier de ses réunions statutaires) des situations suivantes si elles se présentent :
   - de **toute modification au projet,** comme il a été approuvé en ce jour, qui comporterait des changements dans le choix des participants, dans le recrutement, dans la manière d'obtenir leur consentement, de réaliser la collecte des données ou encore, dans les risques ou inconvénients encourus par la participation, et ce, préalablement à l'application de ce changement (modèle de lettre de demande d'amendement disponible sur le site Internet des CÉRUL) ;
   - de **toute modification** qui serait apportée à un **instrument utilisé pour le recrutement** (annonces, affiches, etc.), pour confirmer le **consentement** (formulaire de consentement, feuillet d'information, etc.) ou pour effectuer la **collecte** des données (questionnaire, grille d'entrevue, etc.) en fournissant la nouvelle version du document concerné, où les modifications auront été mises en évidence, préalablement à son utilisation ;
   - de **tout événement imprévu et sérieux** (ex. : détresse psychologique d'un participant, menace proférée à l'égard d'une personne, effets secondaires ou imprévus ou indésirables d'un produit, d'un médicament ou d'un test, etc.) qui surviendrait dans le déroulement d'une activité du présent projet et qui impliquerait un participant, en complétant le formulaire VRR-EI disponible sur le site Internet des CÉRUL ;
   - de l'**interruption prématurée de ce projet de recherche** pour une raison quelconque, qu'il soit financé ou non, y compris en raison de la suspension ou de l'annulation de l'approbation d'un organisme subventionnaire.
2. Tant que le projet n'est pas terminé, incluant les publications, présenter annuellement une **demande de renouvellement** de l'approbation, en fournissant un rapport sur le déroulement de la recherche, le nombre de participants recrutés et, le cas échéant, sur les difficultés rencontrées en cours de réalisation, à l'aide du formulaire VRR-107. La demande de renouvellement doit être

Maison Michael-John-Brophy
2241, chemin Sainte-Foy
Québec (Québec) G1V 0A6
CANADA

418 656-2131, poste 4906
Télécopieur : 418 656-2040
cer@vrr.ulaval.ca
www.cer.ulaval.ca

UNIVERSITÉ LAVAL

Vice-rectorat à la recherche et à la création
Comité d'éthique de la recherche

transmise au Comité dans un délai de 30 jours avant la date de fin de l'approbation, indépendamment du calendrier des réunions statutaires.

Maison Michael-John-Brophy
2241, chemin Sainte-Foy
Québec (Québec) G1Y 0A6
Canada

418 656-2131, poste 4506
Télécopieur : 418 656-2040
cer@vrr.ulaval.ca
www.vrr.ulaval.ca

UQÀM CIEREH
Comité institutionnel d'éthique de la recherche avec des êtres humains
Université du Québec à Montréal

Le 7 décembre 2020

Monsieur Traian Toma
École de criminologie
Université de Montréal

Objet : Reconnaissance éthique

Projet de recherche : *L'impact de la cyber-résilience sur la réaction du public à la suite d'une brèche de données chez les entreprises canadiennes*

Équipe de recherche : s/o

No CER UdeM : CERSC-2020-123-D
No eReview UQAM : 4764_e_2020
Financement : s/o

Monsieur,

Au nom du Comité institutionnel d'éthique de la recherche avec des êtres humains, j'accuse réception des documents évalué par le CER de l'Université de Montréal pour le projet cité en objet et transmis au CIEREH en date 2 décembre 2020.

Le Comité considère que le dossier approuvé par le CER-SC de l'Université de Montréal apparait au-deçà du risque minimal et couvre l'ensemble des préoccupations éthiques soulevées par le projet de recherche. En conséquence, le CIEREH reconnaît accepter sans réserve la demande de reconnaissance. Nous notons que le présent certificat d'éthique est valide jusqu'au **1 décembre 2021**.

Nous vous invitons à présenter un rapport de suivi annuel au CIEREH pour transmettre le document attestant de la prolongation de la période de la validité de la certification éthique lorsque vous obtiendrez ce document de la part du CER-SC de l'Université de Montréal.

Le Comité vous remercie d'avance de votre aimable coopération et vous prie de recevoir l'expression de mes sentiments les meilleurs.

Le président,

Yanick Farmer, Ph.D.