Université Walden

Collège de gestion et de technologie

Il s'agit d'attester que l'étude doctorale par

Yawo Obimpe Kondo

a été jugée complète et satisfaisante à tous égards,
et que toutes les révisions requises par
le comité de révision ont été constitués.

Comité de révision

Dr Gail Miles, présidente du comité, Faculté des technologies de l'information
Dr Gary Griffith, membre du comité, Faculté des technologies de l'information
Dr Bob Duhainy, examinateur universitaire, Faculté des technologies de l'information

Directeur des études et prévôt

Sue Subocz, Ph.D.

Université Walden

2021

Abstrait

Les responsables de la sécurité des systèmes d'information (ISSM) dans les organisations à but non lucratif sont confrontés à une augmentation des cas de cyberattaques, car les organisations à but non lucratif utilisent principalement des technologies de base en raison de leur désir de réduire les coûts. Les objectifs de cette étude de cas multiple qualitative étaient d'explorer les stratégies que les ISSM des organisations à but non lucratif emploient pour se protéger contre les cyberattaques. La base de cette étude était la théorie générale des systèmes. Les participants à cette étude comprenaient cinq responsables informatiques et directeurs des technologies de l'information en charge de la gestion de la sécurité dans des organisations à but non lucratif du Maryland, du district de Columbia et de Virginie. Les données ont été générées par le biais d'entretiens et de l'examen de documents d'archives. La recherche a utilisé la vérification des membres pour établir la fiabilité et l'exactitude des résultats. La recherche a établi trois thèmes sur la base de l'entretien et des données d'archives : la sensibilisation à la cybersécurité, la stratégie de cybersécurité et la dépendance à des tiers. Dans l'ensemble, la recherche a identifié différentes stratégies utilisées par les ISSM pour garantir la cybersécurité : planification stratégique de la cybersécurité, procédures et politiques de sécurité, évaluations régulières de la cybersécurité, formation à la sensibilisation à la sécurité, pratiques de sécurité standard, opérations tierces et examen minutieux de la sécurité physique. De plus, la recherche a énuméré des recommandations que les ISSM peuvent utiliser pour mettre en œuvre des stratégies de cyberattaque pour les organisations à but non lucratif. Les implications positives de cette recherche sur le changement social

incluent la transmission de stratégies de cybersécurité efficaces pour les ISSM à but non lucratif afin d'atténuer et de prévenir les attaques potentielles de cybersécurité, renforçant ainsi les missions des organisations à but non lucratif.

Stratégie de cyberattaques pour les organisations à but non lucratif

par

Yawo O. Kondo

MS, Université Walden, 2018

MS, Université du Maryland Université Collège, 2011

BA, Université du Nebraska à Omaha, 2006

Étude doctorale soumise en réalisation partielle

des Exigences pour le Diplôme de

Docteur en technologie de l'information

Université Walden

Mars 2021

Dévouement

Je souhaite dédier l'étude de recherche au Dieu Tout-Puissant, qui m'a donné la lumière et la force pour mener la recherche. Je dédie également mes recherches à mes parents Kondo Kokou Eloi et Allado Miekuna. Merci, maman, de vous efforcer de nous montrer à tous l'essence de la lutte, de l'intégrité et de l'humilité dans tous les aspects de notre vie. A ma soeur Kokoe, je t'aime plus que tu ne le penses. À ma défunte sœur Enyonamvi, il n'y a pas de jour sans que je pense à toi depuis que tu es décédé. À mes enfants Lauren et Seyram rêvent et cultivent l'humilité, ayez soif de connaissances, faites confiance à votre voix intérieure et n'abandonnez jamais même lorsque les choses deviennent difficiles. Merci, Cecilia, d'être là quand j'étais occupée avec les lectures. À mes frères et sœurs pour m'avoir toujours poussé à être une meilleure personne.

Remerciements

Je tiens à remercier les membres du comité qui ont contribué à faire en sorte que je termine mon projet comme souhaité. En particulier, je remercie le Dr Miles, dont les travaux m'ont encouragé et guidé tout au long de ce voyage. Je remercie également Dr Griffith et Dr Duhainy, pour les nombreuses suggestions tout au long de ce projet d'étude. Je suis reconnaissant envers mes proches, Team Forever, Kaga, Anna Williams, Affi, amis et collègues qui, tout au long du processus d'étude, m'ont encouragé à chaque étape du programme DIT. Je suis très reconnaissant pour vos pensées, vos prières et vos vœux. Enfin, merci aux participants à cette recherche d'avoir pris le temps, malgré leur emploi du temps chargé, de me rencontrer et de faire de l'étude un succès.

Sommaire

List of Tables

Section 1 : Fondement de l'étude

Contexte du problème

Dans le passé, beaucoup considéraient les cyberattaques comme s'il s'agissait d'un problème qui ne touchait que les organisations à but lucratif. Cependant, l'augmentation des cas de cyberattaques parmi les organisations à but non lucratif continue d'affecter leurs opérations et même leur existence (Carrapico et Farrand, 2017). Selon Romanosky (2016), jusqu'à 3% des organisations à but non lucratif signalent des cas de données volées ou perdues. Cependant, les entreprises à but non lucratif rencontrent des taux de litiges relativement faibles de 9 % (Romanosky, 2016). Les données probantes tirées de l'étude ont souligné que même si les dirigeants reconnaissent l'existence des cyberattaques et expriment des préoccupations en matière de cybersécurité, il existe un écart important entre l'inquiétude et la prise de mesures (Romanosky, 2016).

Plusieurs aspects du fonctionnement des organisations à but non lucratif exposent leur vulnérabilité aux cyberattaques. Par exemple, les organismes sans but lucratif préfèrent une technologie rudimentaire qui peut être liée au désir de réduire les coûts opérationnels, comme l'utilisation d'ordinateurs donnés, d'anciennes versions de logiciels non prises en charge et même de systèmes d'exploitation désuets (Bauer et coll., 2017). Plus un système se développe tôt, plus il devient vulnérable aux violations de données. De plus, les organisations à but non lucratif utilisent couramment des logiciels open source comme moyen d'économiser sur les coûts. La décision d'utiliser un logiciel open source augmente la vulnérabilité aux cyberattaques par rapport à l'utilisation d'une

version propriétaire (Bauer et coll., 2017). De nombreuses petites organisations à but non lucratif ne peuvent pas maintenir de personnel dédié aux technologies de l'information (TI) pendant des périodes plus longues. Le manque de personnel informatique dédié les expose à des pirates informatiques qui profitent de la situation pour violer leurs données (McMahon et al., 2015).

Énoncé du problème

La mise en œuvre de l'informatique dans les organisations à but non lucratif est un défi qui affecte la confidentialité, l'intégrité et la vie privée malgré l'augmentation des cyberattaques (Garlinec et al., 2017). Les rapports d'incidents d'atteinte à la protection des données indiquent une multiplication par quatre entre 2005 et 2014, passant d'un peu plus de 200 à plus de 1 200 incidents, ce qui signifie que les incidents de cybersécurité sont à la hausse pour les organismes sans but lucratif (Romanosky, 2016). Le problème informatique général est que les organisations à but non lucratif sont régulièrement confrontées à des risques de sécurité. Le problème informatique spécifique est que certains responsables de la sécurité des systèmes d'information (ISSM) dans les organisations à but non lucratif manquent de stratégies pour se protéger contre les cyberattaques.

Énoncé de l'objet

L'objectif de cette étude de cas qualitative multiple était d'explorer les stratégies que les organisations à but non lucratif emploient pour se protéger contre les cyberattaques. La population spécifique comprenait des responsables informatiques et des directeurs informatiques en charge de la gestion de la sécurité dans des organisations à

but non lucratif du Maryland, du district de Columbia et de Virginie. J'ai mené l'étude à différents endroits en utilisant les informations des participants. L'implication du changement social de cette étude est que les personnes responsables ou engagées avec des organismes à but non lucratif qui peuvent réduire le vol d'identité et créer des environnements plus sûrs. L'impact du changement social peut être considérable parce que les victimes de cyberattaques subissent des pertes financières, des perturbations opérationnelles, des dommages à la réputation et des ramifications juridiques, entre autres effets néfastes. Avec la nature omniprésente des cyberattaques, de nombreuses personnes souffrent de données volées et mal utilisées.

Nature de l'étude

J'ai sélectionné l'étude de cas qualitative multiple pour cette recherche. Un chercheur qualitatif découvre et explore en profondeur des significations et des interprétations couvrant des expériences de vie individuelles concernant un phénomène (Daher et al., 2017). La pertinence de la méthode qualitative réside dans son potentiel d'exploitation pour enquêter sur les technologies, les pratiques et les politiques utilisées dans le cadre des stratégies des ISSM auprès d'organisations à but non lucratif pour se protéger contre les cyberattaques. La méthode quantitative permet à un chercheur d'examiner la relation entre les variables indépendantes et la variable dépendante pour explorer et décrire une situation (Grimaldo et coll., 2018). Je n'ai pas choisi la méthode quantitative parce que je n'ai pas testé d'hypothèses ou de théories ou de statistiques d'examen. L'utilisation d'une approche fondée sur des méthodes mixtes aurait nécessité le couplage des méthodologies qualitatives et quantitatives, ce qui aurait inclus la mise à

l'essai d'hypothèses (Snelson, 2016). Comme je n'ai pas testé d'hypothèses, j'ai jugé que l'approche des méthodes mixtes n'était pas appropriée pour mon étude.

La conception d'une étude de cas met l'accent sur l'apprentissage approfondi d'une situation donnée afin de restreindre un vaste domaine de recherche pour établir un sujet facile à étudier (Margaret, 2016). J'ai choisi une étude de cas multiple pour examiner plusieurs cas afin de comprendre les similitudes et les différences des stratégies de sécurité informatique dans les organisations à but non lucratif. D'autres options comprenaient la conception ethnographique, qui est basée sur une étude approfondie et l'explication d'un lieu particulier et sa culture, les gens, la structure sociale, et les comportements (Bamkin et al., 2016). Je n'ai pas choisi la conception ethnographique parce que mon but n'était pas de mener une étude culturelle. Le modèle phénoménologique détermine principalement une expérience vécue basée sur une philosophie (Mayoh &Onwuegbuzie, 2015). Je n'ai pas choisi la conception phénoménologique parce que mon objectif n'était pas de comprendre une expérience vécue unique.

Une étude de cas constitue une enquête empirique sur un phénomène contemporain qui se produit dans un contexte réel, principalement lorsque la distinction entre le contexte et le phénomène n'est pas claire (Yin, 2017). L'adoption de la conception de la recherche de l'étude de cas nécessite la collecte impartiale de données à partir de situations réelles et la détermination de réponses sur le comment, le quoi et le pourquoi des données (Yin, 2017).

Question de recherche

RQ : Quelles sont les stratégies que les ISSM des organisations à but non lucratif emploient pour se protéger contre les cyberattaques ?

Questions d'entrevue et de sondage

1. Comment évaluez-vous les violations de données dans votre organisation pour savoir si l'organisation réussit à les contenir ou si elles deviennent incontrôlables ?

2. Entre les violations de données internes et externes, lesquelles affectent le plus votre organisation et pourquoi ?

3. Quelles stratégies utilisez-vous pour vous assurer que votre personnel informatique est qualifié pour traiter les failles de sécurité ? Pourquoi ou pourquoi pas ?

4. Quelles stratégies employez-vous pour vous assurer que votre service informatique dispose de budgets adéquats pour traiter les violations de données ? Pourquoi ou pourquoi pas ?

5. Votre organisation sensibilise-t-elle les employés à la sécurité grâce à des programmes spéciaux mis en œuvre par le gestionnaire du SI ?

6. Quelles procédures votre organisation met-elle en œuvre pour effectuer des audits de conformité internes dans le cadre des stratégies utilisées pour protéger les informations contre les cyberattaques ?

7. Quels processus de sécurité des données votre organisation met-elle en œuvre pour se protéger contre tout accès non autorisé aux réseaux de l'organisation ?
8. À quelle fréquence votre organisation forme-t-elle son personnel aux meilleures pratiques en matière de sécurité informatique ? Pensez-vous que cela suffit, et pourquoi ou pourquoi pas ?
9. Quelle est l'étendue de l'automatisation des processus dans votre organisation en ce qui concerne les stratégies utilisées pour protéger les informations contre les cyberattaques ?
10. À quelle fréquence votre organisation rejette-t-elle périodiquement les renseignements personnels à sa disposition qui ne sont plus nécessaires dans le cadre d'une stratégie visant à protéger les renseignements contre les cyberattaques ?
11. Quelles sont les procédures adoptées par votre organisation pour éliminer les renseignements personnels qui ne sont plus nécessaires pour protéger les renseignements contre les cyberattaques ?
12. Selon vous, quelles stratégies votre organisation devrait-elle adopter pour améliorer la sécurité informatique ?

Cadre conceptuel

J'ai utilisé une théorie générale des systèmes (GST) pour mon cadre conceptuel. Von Bertalanffy est l'auteur de GST en 1968, et ses prémisses étaient que les systèmes

complexes partagent les mêmes principes d'organisation qui peuvent être déterminés et modélisés mathématiquement (Kristof et al., 2019). Il s'agit d'une théorie générale qui comprend la science des systèmes, la technologie des systèmes et la philosophie des systèmes (Verhoeff et al., 2018). La philosophie principale de la TPS est fondée sur la façon dont le système fonctionne ensemble et sur la façon dont une partie du système permet de comprendre les autres parties. Chen et coll. (2012) ont décrit ce niveau d'interactions coopératives et de relations continues au sein du système comme étant holistique. Rousseau et al. (2018) a décrit plus en détail le système général comme un système complet ou un stade d'organisme naturel sans altération.

Bien que les progrès technologiques aient contribué à de nouvelles innovations commerciales, ils constituent également des menaces pour les organisations en ce qui concerne la possibilité accrue de perdre leurs précieuses informations. Ces défis nécessitent des approches holistiques qui englobent la collaboration et l'interrelation pour atteindre les objectifs de sécurité (von Bertalanffy, 1972). Dans la présente étude, l'application de la TPS consistait à utiliser les divers sous-systèmes (intrants) pour produire un résultat sûr (extrant). Les cyberattaques augmentent lorsqu'il n'y a pas d'harmonie entre les politiques, les logiciels, le matériel et la formation. L'application de l'approche de la TPS de von Bertalanffy à l'étude m'a aidé à évaluer comment les sous-systèmes fonctionnent les uns avec les autres.

Définition des termes

Cloud : paradigme de calcul comprenant cinq caractéristiques critiques du libre-service à la demande, du pool de ressources, de l'accès étendu au réseau, de l'élasticité

rapide et des services mesurables. L'infonuagique existe également dans trois modèles de services différents : la plateforme en tant que service, le logiciel en tant que service et l'infrastructure en tant que service (Marchisotti et al., 2019).

Cyberattaque : Dommages et atteintes aux données numériques attribués à l'exploitation et à l'application illégales de renseignements confidentiels et personnels (Meisner, 2018).

Cybersécurité : Domaine de politique axé sur la gestion des cybermenaces, y compris les perturbations, l'accès non autorisé et la modification de l'information, du matériel, des logiciels, des réseaux et des services stockés électroniquement (Yost, 2016).

Violation de données : situations où des parties externes ont accès sans autorisation à un grand volume de données client confidentielles, telles que des informations de carte de crédit, d'adresse, etc. L'accès non autorisé provient souvent de personnes, à l'intérieur ou à l'extérieur de l'entreprise, qui cherchent à exploiter des logiciels non sécurisés ou erronés, à altérer ou à voler du matériel et à introduire des logiciels malveillants dans les systèmes (Kude et coll., 2017).

Chiffrement : Mécanisme utilisé pour masquer intentionnellement les données de personnes non autorisées qui peuvent les utiliser de manière involontaire et causer des problèmes de sécurité. Le chiffrement masque les données à l'aide d'algorithmes spécifiques (El-Bendary, 2017).

Pare-feu : matériel ou logiciel essentiel utilisé entre deux réseaux ou plus qui appliquent le contrôle d'accès. Un pare-feu garantit la sécurité du réseau lorsqu'il passe

au crible toutes les données entrantes et sortantes pour s'assurer que seules les données pertinentes et sécurisées sont autorisées (Alabady et al., 2018).

Malware : abréviation de malicieux logiciel. Les logiciels malveillants ciblent les ordinateurs et les utilisateurs d'ordinateurs en corrompant des fichiers, en volant des informations ou simplement en introduisant des activités malveillantes qui agacent les utilisateurs (Tahir, 2018).

Hypothèses, limites et délimitations

Hypothèses

Selon Wolgemuth et coll. (2017), les hypothèses de recherche constituent des idées qu'un chercheur accepte comme exactes, même si cette même position peut ne pas être étayée par des faits. En tant que chercheur pour cette étude doctorale, j'avais les hypothèses suivantes. J'ai supposé que l'examen des documents des organismes sans but lucratif et les entrevues avec les gestionnaires organisationnels des organismes sans but lucratif fournissaient des données adéquates pour répondre à la question de recherche. J'ai supposé que les participants à la recherche offrissent des réponses honnêtes qui aideraient à améliorer la validité de l'étude.

Limitations

Les limites de recherche d'une étude particulière font référence aux faiblesses potentielles indépendantes de la volonté du chercheur et sont étroitement associées à la conception de la recherche, aux contraintes de financement, aux contraintes du modèle statistique et à d'autres facteurs (Theofanidis et Fountouki, 2019). Le nombre de participants que j'ai interviewés dépendait du nombre d'organisations à but non lucratif

disponibles dans le Maryland, le district de Columbia et la Virginie. De plus, la politique organisationnelle concernant la divulgation d'informations considérées comme internes et privées a limité mon accès à des données qui auraient pu être pertinentes.

Délimitations

Les délimitations de recherche constituent les définitions que le chercheur choisit de fixer, signalant les limites ou les limites de son travail de sorte que les objectifs et les buts de l'étude deviennent pratiquement réalisables (Theofanidis &Fountouki, 2019). Contrairement aux limitations qui échappent au contrôle du chercheur, avec des délimitations, le chercheur est entièrement en contrôle (Korrapati, 2016). Les facteurs délimitant comprennent les questions de recherche, le choix des objectifs, les perspectives théoriques adoptées, la population à l'étude et les variables d'intérêt (Wolgemuth et coll., 2017). La qualité de toute recherche reflète la capacité du chercheur à gérer efficacement les préjugés personnels. La haute qualité aidera à présenter des données de recherche objectives (Wolgemuth et coll., 2017). La délimitation de cette étude était qu'elle impliquait des organisations à but non lucratif présentant les caractéristiques suivantes : a) organisations autorisées à opérer légalement dans l'État du Maryland et le district de Columbia; b) les organisations comptant au moins 150 personnes; c) les organisations qui ont mis en œuvre efficacement des mesures de cybersécurité et d) les organisations dont les recettes annuelles brutes s'élèvent à au moins 5 millions de dollars. Les organismes sans but lucratif qui ne répondaient pas aux critères ci-dessus n'ont pas participé à l'étude.

Importance de l'étude

Le but de cette étude était d'explorer les stratégies que certains ISSM dans les organisations à but non lucratif utilisent pour se protéger contre les cyberattaques. Les résultats de la recherche pourraient aider les responsables informatiques et les directeurs informatiques à protéger leurs organisations contre les menaces de cybersécurité. Pour les organisations informatiques, l'étude pourrait fournir des informations qu'elles peuvent utiliser pour améliorer la cybersécurité dans leurs locaux et aider à garantir la confiance des clients. Cette étude pourrait être utile aux dirigeants principaux de l'information (DSI) et aux dirigeants principaux de la sécurité de l'information (RSSI) pour élaborer les stratégies dont ils ont besoin pour protéger leurs renseignements. Les constatations pourraient également aider les gestionnaires de la TI et les directeurs de la TI à élaborer un plan d'action pour atténuer l'effet des cybermenaces sur leur rendement.

De plus, l'information pourrait aider les responsables informatiques à développer une formation interne sur la cybersécurité afin d'améliorer la sécurité des données dans l'organisation. Les organisations à but non lucratif exposent par inadvertance leurs actifs à des failles de sécurité, tout comme les organisations à but lucratif. Les cybermenaces peuvent affecter la productivité et les finances d'une organisation. Grâce aux conclusions de cette étude, les praticiens de l'informatique peuvent disposer d'outils pour développer des stratégies de cybersécurité efficaces afin de protéger les données dans les organisations à but non lucratif. Les employés peuvent participer à des campagnes d'alphabétisation sur les cybermenaces où ils transfèrent leurs connaissances aux membres de la communauté. Une telle expérience peut donner lieu à une compréhension

générale des cybermenaces et, à ce titre, à une communauté plus sûre en ce qui concerne la cybersécurité.

En termes de changement social, Bach-Mortensen et Montgomery (2018) ont observé que les organismes sans but lucratif occupent une position critique dans la société parce qu'ils fournissent des services ou des produits précieux à la communauté, ciblant des groupes vulnérables tels que les personnes âgées, les personnes handicapées, les enfants et les jeunes à risque. Selon le National Council of Nonprofits (2016), les organisations à but non lucratif fournissent des services sociaux essentiels, tels que des abris, de la nourriture et des interventions d'urgence, bénéficiant à des millions d'Américains. Dans cette étude, j'ai cherché à mettre en évidence les stratégies de cybersécurité critiques qui peuvent aider les dirigeants des organisations à but non lucratif à s'assurer que leurs systèmes et leurs documents internes sont à l'abri des pirates. Avec la sécurité accrue du système, les organisations à but non lucratif pourraient protéger les données sur leurs bénéficiaires, y compris les personnes âgées, les personnes handicapées, les enfants et les jeunes, protégeant ainsi leur vie privée.

Un examen de la littérature professionnelle et universitaire

Une revue de la littérature est un aspect essentiel de toute recherche, car le chercheur l'utilise pour s'appuyer sur des études antérieures et sur la base de connaissances disponible pour éclairer les recherches les plus récentes (Boell et Cecez-kecmanovic, 2015). L'objectif de cette recherche nécessitait d'étudier les stratégies de cyberattaque utilisées efficacement par les organisations à but non lucratif pour protéger leurs données. J'ai utilisé la revue de la littérature pour atteindre cet objectif en

fournissant des détails factuels sur le sujet d'intérêt tels que rapportés par les chercheurs qui ont étudié et mené des recherches dans ce domaine. Le cadre conceptuel que j'ai choisi pour l'étude était le déterminant du choix des sources de la littérature. La GST, dont von Bertalanffy est l'auteur en 1968, a été le fondement de l'étude. Les sources documentaires examinées dans les présentes études ont exploré les sujets liés à la TPS et les théories alternatives qui les comparaient ou les contrastaient.

Pour cette recherche, j'ai puisé dans diverses ressources, notamment IEEE Source Library, ProQuest, EBSCOhost, Google Scholar, des sites Web gouvernementaux et Science Direct. J'ai tricoté le sujet de recherche, qui était des stratégies de sécurité informatique utilisées pour protéger les informations contre les cyberattaques contre les organisations à but non lucratif, en utilisant des termes de recherche tels que les stratégies de sécurité informatique contre les *cyberattaques dans les organisations à but non lucratif, les stratégies de sécurité des cyberattaques dans les organisations à but non lucratif américaines* et les stratégies de protection *de l'information dans les organisations à but non lucratif.* Étant donné que l'informatique est un domaine universitaire en pleine croissance, les documents littéraires plus anciens ont tendance à perdre de leur pertinence avec le temps. J'ai donc concentré cette revue de littérature sur des sources plus récentes publiées entre 2015 et 2020. J'ai rassemblé 165 sources différentes pour la revue de la littérature, dont 98% étaient des articles évalués par des pairs. Jusqu'à 96 % des 165 sources ont été publiées en 2015 ou après. Dans l'ensemble, la revue de la littérature offre une analyse critique de la question d'actualité déterminée par la question de recherche. L'analyse documentaire est structurée en quatre domaines

principaux afin de permettre une discussion logique. Ces quatre sections comprennent le cadre conceptuel, qui fournit une explication complète de la théorie originale de la TPS et de son évolution, des approches à l'appui et contrastées, et d'autres études qui s'harmonisent avec les diverses méthodes. Les sections de revue de la littérature traitent de l'atteinte à la protection des données, de la gouvernance des données, de la sécurité et de la protection de la vie privée.

Théorie générale des systèmes

Von Bertalanffy a instauré la TPS en 1968 ; il y décrit le monde comme étant basé sur des systèmes irréductiblement intégrés. Sa découverte a offert un cadre sur lequel fonder les aspects fondamentaux des disciplines et des enjeux dans un corpus de connaissances systématique et raisonné (Drack &Pouvreau, 2015). Dans le passé, la science se concentrait sur l'explication des phénomènes observables en les décomposant en une interaction entre des unités élémentaires pouvant être étudiées séparément (Bertalanffy, 1968). Selon Bertalanffy (1968), cet accent diffère des concepts scientifiques contemporains, qui sont plus sur la « plénitude », ce qui est quelque peu vague. La science moderne se concentre donc sur les problèmes d'organisation, les interactions dynamiques visibles dans la disparité de comportement des parties existant isolément ou dans un arrangement supérieur, etc. Les conceptions et les questions de cette nature sont communes à toutes les branches scientifiques, qu'il s'agisse de choses inanimées, de phénomènes sociaux ou d'organismes vivants qui font l'objet d'études (Bertalanffy, 1968).

La TPS sert à déterminer l'intégralité ou la totalité des problèmes scientifiques et sociaux (Bridgen, 2017). L'objectif sous-jacent de l'application de la TPS est d'atteindre un cadre méta scientifique grâce à la systéologie générale, ce qui a entraîné une intégration indispensable dans l'enseignement scientifique (Drack et Pouvreau, 2015). Une telle approche exacte est cruciale dans les domaines non physiques de la science. Cette théorie est plus proche de l'unité de l'objectif de la science, car elle se développe sur des principes courants « verticalement » dans tout l'univers des sciences séparées (Bertalanffy, 1968). Essentiellement, le concept de TPS s'est aligné sur l'objectif de cette étude, car les cyberattaques constituent des problèmes scientifiques et sociaux qui affligent les organisations à but non lucratif à travers les États-Unis. L'exploration des stratégies utilisées par les ISSM dans les organisations à but non lucratif pour se protéger contre les cyberattaques atteint un cadre méta-scientifique grâce à la systéologie générale.

Selon Schneider et coll. (2016), la TPS est une façon de penser plus ciblée qui prend une vision du monde comme proportion. En tant que système ouvert, l'organisation interagit de manière persistante avec son environnement local en échangeant des « matériaux » (Schneider etal., 2016). De plus, l'organisation interagit également avec les éléments de l'environnement externe (Turner &Baker, 2019). Bien que chacun de ces systèmes sociaux présente des caractéristiques non matériales distinctes, ils correspondent tous à la composition de base des systèmes ouverts vivants. La TPS est davantage liée aux uniformités qui contribuent à leurs processus et à leurs principes de fonctionnement qu'à leurs similitudes structurelles (Kordova et coll., 2018). Comme

Schneider et coll. (2016) l'ont expliqué, la TPS est utilisée pour rechercher des concepts fondamentaux plus pertinents pour tous les systèmes.

L'importance de la TPS en tant que théorie fondamentale de cette recherche réside dans le fait que de nombreux organismes à but non lucratif ont intégré leurs opérations dans des ordinateurs et des systèmes informatiques. Il est possible que les activités de ces organismes de bienfaisance cessent lorsque des personnes malveillantes piratent des ordinateurs et des réseaux informatiques. Cette menace fait face à pratiquement toutes les organisations qui dépendent fortement des processus informatisés (Posey et coll., 2017). La réalité de cette menace résulte souvent du fait que de nombreuses organisations à but non lucratif n'investissent que dans des systèmes informatiques de base facilement empiétés sur pour que leurs opérations soient affectées par des pirates. Dans de tels cas, les organisations à but non lucratif finissent par perdre des données cruciales. Néanmoins, le concept de TPS peut aider à changer la norme dans la façon dont les organismes à but non lucratif fonctionnent en proposant spécifiquement de meilleurs systèmes organisationnels qui améliorent l'efficacité. La théorie fondamentale de la TPS suggère des systèmes supérieurs qui s'avéreront difficiles à manipuler facilement par des pirates informatiques, ce qui entraînerait une désorientation du service.

Évolution du système général

Plusieurs chercheurs ont continué à examiner la théorie de la TPS de von Bertalanffy dans le but de l'élargir pour créer un sens plus élaboré. Au fur et à mesure de l'évolution de la TPS, les chercheurs ont transformé la méthode en un domaine d'étude

interdisciplinaire impliquant différents concepts, principes et modèles. Les nouvelles approches des systèmes théoriques, telles que la cybernétique, la théorie du contrôle, la théorie des automates, la théorie de l'information, les mathématiques relationnelles, la théorie des ensembles, des graphes et des réseaux, l'informatisation et la simulation, et la théorie des jeux et de la décision, ne relèvent pas de la GST (Von Bertalanffy, 1972). Néanmoins, la TPS et la théorie des systèmes sont considérées comme la norme des domaines pour plusieurs autres disciplines des sciences sociales. Ces nombreuses approches systémiques théoriques, selon Von Bertalanffy (1972), sont liées à des problèmes systémiques.

L'examen des progrès de la théorie des systèmes au fil du temps montre une variété d'activités intellectuelles et un effort pratique. La première particularité du domaine général de travail sur la théorie des systèmes réside dans l'expansion des idées de systèmes pour elle-même (comme la cybernétique) et l'application des idées de systèmes dans une discipline donnée (Krippner et al., 1985). Dans la branche qui se concentre sur les travaux au sein des sciences des systèmes, il existe une distinction entre l'avancement purement hypothétique des idées de systèmes et leur interrelation et l'effort pour développer des idées de systèmes considérées comme importantes dans l'interprétation ou la manipulation de conditions du monde réel (Moore et al., 2017). Néanmoins, d'autres exemples conduisent à une triple distinction, y compris les approches systémiques rigides (par exemple, celles employées en génie des systèmes), les approches systémiques douces (par exemple, celles adoptées en psychologie humaniste),

ainsi que les approches systémiques hybrides (par exemple, celles utilisées dans la recherche opérationnelle pour faciliter la prise de décision).

Selon Muegge et Craigen (2015), la théorie générale des systèmes offre une base importante pour aborder efficacement la cybersécurité. En utilisant l'argument de Muegge et Craigen, Ogliastri et coll. (2016) ont appuyé leur point de vue en démontrant l'applicabilité de l'approche de la TPS dans le cas des organismes sans but lucratif et leur gestion des données pour prévenir les atteintes à la protection des droits. L'examen de certaines des stratégies efficaces employées par les organismes sans but lucratif pour se protéger contre les cyberattaques peut offrir les meilleures pratiques, renforcer la confiance des consommateurs et inspirer la prospérité économique (Ogliastri et coll., 2016). Ces stratégies ont servi de base à cette étude pour explorer les stratégies de sécurité informatique utilisées pour protéger les informations contre les cyberattaques contre les organisations à but non lucratif.

Soutenir les Théories

Selon Horne et coll. (2016), il n'existe aucune théorie apparente sur la sécurité de l'information. Une théorie plus forte, comme Horne et coll. (2016) l'ont également soutenu, peut être obtenue en reliant les théories de types variés. Horne et coll. (2016) ont convenu qu'il existe plusieurs théories liées à la sécurité de l'information, comme la théorie de la guerre de l'information (TIW) et la théorie de la motivation de la protection (TPM), mais ils ont noté qu'aucune de ces théories n'est axée sur la seule sécurité de l'information. La gestion des risques liés à la cybersécurité augmente également la

probabilité qu'une organisation atteint ses objectifs en maximisant les possibilités qui peuvent se présenter (Garlinec et coll., 2017).

Théorie de la guerre de l'information

Le TIW, comparé à la TPS, est un cadre relativement nouveau dont l'origine est attribuée à Sun Tzu (512 avant notre ère), à la suite du grand saut dans les technologies de communication ainsi que dans Internet (Baskerville,2010). La communication et les progrès technologiques ont eu des conséquences stratégiques touchant les gouvernements, les forces armées et la population en général (Monov et Karev, 2018). Aujourd'hui, les multiples noms utilisés pour la guerre de l'information représentent de nombreuses dimensions et des fins diverses. Selon Libicki (2017a), dans le contexte des technologies modernes, tiw comprend des moyens sophistiqués de messagerie, représentant un certain niveau de guerre limitée portant un faible niveau d'escalade tout en offrant des possibilités d'objectifs de progrès géopolitique à un coût minimal. Libicki (2017a) a constaté que la guerre de l'information relève d'un type de menace transnationale, affectant principalement la sécurité nationale, pénétrant dans les frontières nationales et affaiblissant la stabilité. Monov et Karev (2018) ont souligné que tiw est plus sur l'influence sur les dirigeants et la population et le contrôle sur les actions et les décisions. Compte tenu de l'analyse ci-dessus, TIW n'était pas un cadre approprié pour la stratégie de cyberattaques pour les organismes à but non lucratif. Cette théorie est principalement pertinente lorsque des aspects de sécurité nationale touchant les gouvernements et les forces armées sont en jeu.

La théorie de la gestion protectrice

La théorie de la gestion protectrice (PMT), quant à elle, met l'accent sur l'étendue de la gravité des événements nocifs, la susceptibilité perçue à la menace (comme la probabilité de sa survenance), les préoccupations concernant le risque et la disponibilité et l'efficacité d'une intervention d'adaptation pour réduire ou éradiquer l'événement nuisible potentiel (Clubb et Hinkle, 2015). Rogers (1975) était le théoricien original du PMT, et l'hypothèse sous-jacente de sa théorie est que les appels de la peur pourraient causer des changements d'attitude. L'objectif de PMT était d'en supprimer les modèles d'intervention capables de produire des conséquences néfastes ou de créer des modèles d'intervention qui pourraient contrecarrer la survenue d'événements délétères (Rogers, 1975). Les processus cognitifs individuels influencent les effets résultants de ces facteurs de soutien ou de dissuasion. La PMT et la TPS présentent des similitudes en ce sens que les deux sont des théories sociales. Cette similitude signifie qu'ils offrent des idées, des arguments, des hypothèses, des spéculations explicatives et des expériences de pensée concernant les sociétés humaines et les éléments ou structures qui composent ces sociétés. Dans des études récentes entreprises par Wong et coll. (2016) sur le concept de TMP, l'opinion exceptionnelle était que les facteurs individuels et environnementaux peuvent offrir un soutien ou une dissuasion à la pratique de comportements protecteurs. Rajendran et coll. (2017) ont notamment confirmé l'application généralisée de PMT dans la politique de sécurité des systèmes d'information. Par exemple, ils mentionnent un modèle de proposition qui offre des explications sur la conformité des employés en matière de sécurité. Ce modèle est utile pour la cybersécurité, d'autant plus qu'il permettrait aux employés d'organisations, telles que les organisations à but non lucratif,

d'adhérer à un ensemble de comportements qui les dissuaderaient d'aider les violations de données dans l'organisation (Rajendran et al., 2017). Bien que pmt a été appliqué principalement dans la politique de sécurité des systèmes d'information, je n'ai pas choisi la théorie pour cette étude parce qu'il se concentre davantage sur les conséquences du défi. Elle porte sur l'étendue de la gravité des événements nuisibles, la vulnérabilité perçue à la menace et les préoccupations concernant le risque. Cet objectif n'est pas cohérent avec l'objectif de cette étude, qui était d'explorer la stratégie de cyberattaques pour les organisations à but non lucratif afin de protéger les données des pirates.

Les principes de la théorie de la motivation de protection

Les principes du TPM utilisent une perspective sociale pour concevoir des stratégies sur lesquelles des organisations telles que des organismes à but non lucratif peuvent s'appuyer pour établir une protection adéquate contre les cyberattaques (Sommestad et al., 2015). Selon Barlette et coll. (2017), la MPT peut prédire efficacement la volonté d'une personne d'utiliser des comportements protecteurs en ce qui concerne les applications de cybersécurité. Barlette et coll. ont fait valoir que l'utilisation du TPM pourrait aider à tester les facteurs expliquant les intentions comportementales et le comportement réel des gestionnaires dans les organisations, telles que les organisations à but non lucratif, en s'engageant dans des mesures défensives de sécurité de l'information. Doherty et Tajuddin (2018) étaient d'accord avec les observations de Barlette et coll., notant que les praticiens et les gestionnaires peuvent faire face aux défis de la cybersécurité en encourageant leurs collègues à identifier et à considérer leurs informations comme une ressource précieuse. Cette approche permettra

aux organismes sans but lucratif d'améliorer leur conformité aux protocoles de sécurité de l'information (Doherty, &Tajuddin, 2018).

Comparativement, la TPS aborde le discours de la stratégie de cybersécurité du point de vue de l'intégration des systèmes, où l'organisation doit avoir un mélange de stratégies pour garantir la sécurité des données (Kordova et al., 2018). Doherty et Tajuddin (2018) ont estimé que l'approche systémique générale visant à sécuriser les données organisationnelles était préférable à la persuasion des employés à respecter les politiques de sécurité de l'information et à les éduquer sur l'importance de leur traitement de l'information. Selon Doherty et Tajuddin (2018), les organismes à but non lucratif peuvent former leurs employés pour renforcer leur volonté de prendre les mesures nécessaires pour protéger les données. Kim et Kim (2017) ont fait valoir que si les organismes à but non lucratif souhaitent atteindre le plus haut niveau de comportement de conformité parmi leurs employés, il doit y avoir une culture matérielle et une infrastructure soutenant la conformité. Les organismes sans but lucratif doivent également promouvoir les systèmes de conformité en général pour encourager les employés à faire des efforts volontaires.

Une autre théorie à l'appui de la TPS et de son application est la théorie cybernétique ou de contrôle. Cette théorie constitue une approche générale pour comprendre les systèmes d'autorégulation (Theophanidis et al., 2017). Nikolić (2015) a expliqué que les idées centrales de la théorie cybernétique ou du contrôle remontent à 1929 lors de la discussion sur les mécanismes physiologiques homéostatiques. Cependant, Mowlana (2019) a précisé que la naissance de la théorie en tant que corps de

pensée distinct est liée au livre *Cybernetics: Control and Communication in the Animal and the Machine* de Wierner en 1948. Proctor et Xiong (2018) ont soutenu que la cybernétique a préparé le terrain grâce à l'idée que tout, des systèmes neurophysiologiques aux activités sociétales, peut être transformé en systèmes de contrôle structurés constituant des boucles d'avance et de rétroaction. Proctor et Xiong ont en outre découvert que la théorie de l'information fournissait un moyen par lequel l'entropie et l'information peuvent être quantifiées et maintenues en théorisant par le biais du flux d'informations. Proctor et Xiong ont également souligné que la théorie statistique présentait un moyen d'arriver à des inférences scientifiques tirées des résultats d'expériences contrôlées et d'extraire la prise de décision humaine. Ces trois piliers ont marqué l'évolution de la psychologie cognitive à l'ère de l'information (Proctor & Xiong, 2018). Les progrès technologiques à l'ère de l'information ont entraîné un lien accru entre les vies humaines et le cyberespace. Cet entrelacement a, à son tour, fait de la psychologie cognitive un aspect essentiel de la recherche interdisciplinaire en ce qui concerne l'entrelacement (Proctor & Xiong, 2018). Néanmoins, je n'ai pas adopté cette théorie pour cette étude parce qu'elle se concentre davantage sur l'aspect psychologique de l'organisation plutôt que sur une approche globale que j'ai cherché à atteindre avec cette recherche.

Selon Mingers et Standing (2018), la cybernétique ou théorie du contrôle utilise des idées mathématiques simples pour instituer un cadre fondamental pour discuter de la rétroaction, de l'équilibre, de la stabilité, de la perturbation, de l'information, de l'entropie, de la régulation, du bruit, des contraintes et de la transmission

(communication). Du point de vue de la cybernétique, la théorie du système fournit les outils qui se concentrent sur la prise en charge du cycle cybernétique (De Boer &Andersen, 2016). Les points de vue de De Boer et Andersen (2016) coïncidaient avec l'observation de Fal (2016) décrivant la cybernétique comme des mécanismes de rétroaction en boucle fermée avec une sortie qui est directement liée à l'entrée du système subséquent. Selon Drack et Pouvreau (2015), les boucles de rétroaction et les autres canaux de communication qui composent les systèmes peuvent utiliser des relations comportementales au lieu d'une connectivité physique. La description de Drack et Pouvreau capture l'élaboration par Hof (2018) du concept central de la perspective cybernétique en termes d'actions de l'attaquant ou du défenseur ayant un impact sur l'entrée du système rival. Dans cette thèse, cependant, l'accent n'était pas mis principalement sur le fonctionnement des mécanismes de rétroaction des environnements externes à l'organisation et sur leur lien avec les stratégies de cyberattaque. Au lieu de cela, l'accent a été mis sur la façon dont, en tant que système ouvert, l'organisation interagit de manière persistante avec son environnement local en échangeant des « matériaux » et sur la façon dont elle se rapporte à la cybersécurité. La théorie de la TPS illustre la meilleure explication de cette situation, en examinant l'organisation comme un système ouvert qui interagit avec l'environnement externe.

L'application du concept cybernétique dans le scénario d'une organisation prenant en charge les défis de sécurité des données implique qu'un attaquant utilisera la sortie de l'organisation pour modifier sa sortie et affecter négativement les opérations (Pillay, 2017). Selon Pillay (2017), l'attaque pourrait être de n'importe quel type, y

compris l'intrusion ou le déni de service, qui de toute façon finirait toujours par causer un certain niveau d'entrée de perturbation dans le système de l'organisation. Horvath et Lovasz (2018) étaient d'accord avec Pillay (2017), notant que le défenseur s'attendait à détecter les perturbations au sein du système de l'organisation et à tenter d'atténuer ces entrées en utilisant des méthodes telles que l'ajout de pare-feu pour contrôler l'accès au réseau, la réinitialisation de leurs systèmes ou le développement de correctifs. Le cycle se poursuivra indéfiniment, à condition que le défenseur n'agisse qu'en réponse à des perturbations d'entrée reconnues ou détectées (Horvath et Lovasz, 2018). En théorie, la cybernétique propose une structure de contrôle qui facilite la prise de décision au sein du système (Xu et coll., 2016). Le cycle de contrôle primaire constitue un récepteur (capteur ou détecteur) qui enregistre divers stimuli (Xu et coll., 2016). Grâce au mécanisme de rétroaction de surveillance et d'intervention, le système peut parvenir à l'autorégulation (Fal', 2017). Selon Fal' (2017), l'autoréglementation s'appliquerait efficacement dans la structure organisationnelle pour détecter les cyberattaques et fournir des commentaires pour déclencher l'autorégulation.

Théories contrastées

Le point de vue principal de GST selon lequel l'organisation est en interaction constante avec son environnement local par l'échange de « matériaux » va à l'encontre de la position prise par le TPM. Selon le TPM, la volonté d'une personne d'employer des comportements protecteurs est suffisante pour relever les défis de la cybersécurité (Schneider et al., 2016). Selon Kordova et coll. (2018), les lignes directrices de la TPS portent davantage sur les uniformités qui contribuent aux principes de processus et de

fonctionnement des organisations que sur leurs similitudes structurelles. Par conséquent, l'utilisation des principes de la TPS propose de meilleurs systèmes organisationnels qui améliorent l'efficacité de la protection et de la gestion des données dans les organismes sans but lucratif (Posey et coll., 2017).

Le système adaptatif complexe

La théorie du système adaptatif complexe (SAE) a des principes différents de ceux de la TPS. En particulier, le CAS a ses lois sur des systèmes dynamiques ouverts capables d'auto-organiser leur configuration structurelle en utilisant l'échange d'informations, l'énergie, en plus d'autres ressources trouvées dans leur environnement (Coetzee et al., 2016). Les systèmes sont capables de modifier ces ressources pour soutenir l'action, et leur nature auto-organisée n'a que peu ou absolument aucune influence directe sur ces systèmes de la part de forces extérieures (Junior, 2016). La fondation du TAS a eu lieu en 1987 à l'Institut de Santa Fe (SFI), lors de la réunion du SFI qui discutait de la complexité en économie (Citera, 2017). Plusieurs théoriciens sont à l'origine du CAS, y compris des physiciens, des économistes, etc. L'un des théoriciens les plus renommés derrière le CAS était John Henry Holland, qui a conceptualisé un « plan adaptatif » d'évolution génétique, qui modifiait progressivement les structures à l'aide d'opérateurs appropriés (Citera, 2017). Mittal et coll. (2017) ont noté que les plans adaptatifs de Holland ont suscité de l'intérêt pour les méthodes de programmation d'ordinateurs afin d'atteindre des capacités de résolution de problèmes.

Les principes fondamentaux de la SAE comprennent la dynamique non linéaire, l'adaptation/évolution, la théorie du chaos, l'auto-organisation, la rétroaction et le chaos

(Preiser et al., 2018). Ainsi, la perspective cas considère les systèmes basés sur la non-linéarité, ce qui implique que les états futurs sont irréguliers (Preiser et al., 2018). Selon Preiser et al., la transition d'un système de nature simple à complexe entraîne une réduction de la fiabilité des mécanismes prédictifs. Le chaos est déterministe et tout aussi linéaire, et avec une signification mathématique, sensible à ses circonstances initiales (Junior, 2016). Cas implique une modélisation mathématique linéaire et prévisible lors de la visualisation du chaos (Turner &Baker, 2019). L'utilisation de la modélisation mathématique guide le chaos dans l'identification des modèles globaux basés sur les interactions des composants dans la mesure où les systèmes auto-organisés sont impliqués. Selon Shapiro (2015), l'émergence est un élément important de la SAE, car elle se produit lorsque l'interaction des composants du système entraîne de nouveaux états qui contribuent à l'imprévisibilité du système. Les autres principes de rétroaction, d'évolution et d'adaptation font référence à la capacité d'apprentissage d'un système, qui existent tous dans le chaos et cas (Werder &Maedche, 2018).

La SAE contraste avec la TPS en raison d'un système ouvert et fermé (Shapiro, 2015). Selon Shapiro, l'approche des méthodes théoriques s'aligne généralement sur les systèmes fermés, bien que ce ne soit pas toujours le cas. Hodiamont et coll. (2019) étaient d'accord avec Shapiro, soulignant comment plusieurs approches de la TPS considèrent les systèmes ouverts, en particulier ceux qui se concentrent sur les réseaux sociaux. Hodiamont et coll., cependant, soulignent que la SAE s'associe principalement aux systèmes ouverts. Cas est dépeint comme un système non ordonné, complexe et chaotique dans lequel les modèles peuvent faire surface (système ouvert: Reiser et al.,

2018). En revanche, Schneider et coll. (2016) ont souligné l'association de la TPS avec l'arrangement et la pratique des commandes en ce sens qu'il existe des modèles structurés complexes et simples (système fermé). La principale différence entre un système ouvert et un système fermé existe dans la deuxième loi de la thermodynamique qui s'applique principalement à l'ordre fermé (MacDougall, 2019). La deuxième loi de la thermodynamique concerne les approches systémiques théoriques (MacDougall, 2019). Cas oppose la deuxième loi de la thermodynamique en raison de la doctrine de l'auto-organisation et de l'émergence (Adauto & Guerrini, 2018).

La théorie cas est pertinente, en particulier sur la cybersécurité dans les organisations à but non lucratif, car elle reconnaît les problèmes très complexes qui ont émergé en raison de l'utilisation continue de l'informatique dans les organisations. La théorie de la SAE préconise donc une nouvelle approche pour s'attaquer aux espaces décisionnels complexes que les organisations sont devenues (Coetzee et coll., 2016). Selon Törmänen et al. (2016), les principes du CAS ont facilité le type adaptatif intelligent de réponses comportementales systémiques pour répondre à la complexité. Alors que les organismes sans but lucratif font face au grave défi de la perte de données et de la cyber-insécurité, l'approche CAS préconise des systèmes de systèmes destinés à créer un comportement émergent intentionnellement conçu et préféré en utilisant des systèmes constitutifs intelligents et ciblés auto-organisés (Coetzee et al., 2016). Le choix de la TPS plutôt que de la SAE pour cette thèse fait suite à la prise de conscience que la SAE est principalement non ordonnée, complexe et chaotique dans laquelle des modèles peuvent faire surface (système ouvert ; Preiser et coll., 2018). Cette complexité rendrait

difficile de travailler avec lorsqu'on essaie de l'adopter comme base d'explication des stratégies de cyberattaque pour les organismes à but non lucratif. Contrairement aux SAE, cependant, la TPS est en bon ordre. Il existe des modèles structurés compliqués et simples (système fermé ; Schneider et al., 2015), ce qui facilite l'adoption du concept pour expliquer les stratégies de cyberattaque pour les organismes sans but lucratif.

Vulnérabilités des systèmes informatiques à but non lucratif

Les organisations à but lucratif consacrent beaucoup de temps et de ressources à l'amélioration de la sécurité de leurs données, tandis que les organismes sans but lucratif adoptent généralement des politiques inférieures contre la protection et la gestion des données (Gordon et al., 2015). Par exemple, conformément à l'observation de Gordon et al., de nombreux types de recherche ont révélé l'idée fausse parmi les gestionnaires à but non lucratif que leurs organisations ne sont pas aussi à risque pour les pirates que le sont les organismes à but lucratif. Cependant, comme les dernières atteintes à la protection des données l'ont démontré, les organismes sans but lucratif sont tout aussi ciblés par les pirates informatiques que les organismes à but lucratif (Bordoff et coll., 2017). Les organismes sans but lucratif ont souvent des budgets restreints qui sont pour la plupart incapables de financer une évaluation informatique et de contrôle efficace capable d'offrir une meilleure protection (Gordon et al., 2015).

Dans de nombreux cas, les organismes sans but lucratif manquent de personnel dans leurs services informatiques avec les compétences nécessaires pour fournir certaines fonctions spécialisées en cybersécurité (Jalali &Kaiser, 2018). Selon Gordon et coll. (2015), la principale raison de cet événement est que l'objectif principal des organismes

sans but lucratif est de servir des objectifs spécifiques, de travailler à une mission et de concentrer leurs efforts sur l'obtention de financement et la réduction de leurs coûts. La propriété des organisations à but non lucratif, y compris la direction et le personnel, se concentrent toutes sur la réalisation de ces objectifs. Toute leur structure d'incitation définit leur travail vers la réalisation de ces objectifs. Jagalur et coll. (2018); néanmoins, ces objectifs ne sont pas en tandem avec une bonne cybersécurité en général.

De plus, les employés des organismes sans but lucratif ont souvent pensé que la cybersécurité est moins critique parce qu'ils ne considèrent pas leurs organisations comme une cible précieuse pour la cybercriminalité (Almubark et coll., 2016). Bien qu'il n'y ait aucune garantie qu'une stratégie de cybersécurité et des évaluations de sécurité régulières prédiront les menaces dangereuses, la vérité est que les organisations à but non lucratif augmentent leurs chances de limiter l'exposition avec une approche. Une telle stratégie permet aux organisations à but non lucratif de planifier, d'examiner, de tester et d'évaluer leurs faiblesses avant les attaques (Almubark et al., 2016).

Violation de données

Une violation de données est une préoccupation grave à laquelle pratiquement toutes les organisations pensent en raison des dommages potentiels qu'elle laisse dans son sillage. Prakash et Singaravel (2015) ont décrit les atteintes à la protection des données comme des actions organisées visant à extraire des connaissances cachées des collectes de données des gens sans que les gens ne les autorisent. À leur avis, Prakash et Singaravel ont noté que les organisations stockant de nombreuses données sur les personnes peuvent décider d'exploiter ces données dans le but d'apprendre d'autres

tendances individuelles sur les gens, y compris leurs préférences, modèles, modèles, etc. La question de l'atteinte à la protection des données ne se limite pas seulement aux organismes à but lucratif, mais touche aussi beaucoup les organismes sans but lucratif (Levesque et coll., 2015). Holtfreter et Harrington (2015) ont cité un cas qui s'est produit en mai 2006. Un employé frauduleux de la Croix-Rouge a interféré avec la base de données et a accédé à jusqu'à un million de dossiers, dont certains comprenaient des numéros de sécurité sociale de donateurs. Cet incident à la Croix-Rouge américaine correspond à la description de Sen et Borle (2015) d'une violation de données comme un incident où un accès non déclaré à des données sensibles, confidentielles ou protégées se produit. Lorsque cet accès non autorisé se produit, il y a une plus grande probabilité de compromettre l'intégrité, la confidentialité et la disponibilité des mêmes données en question (Sen et Borle, 2015). Bien qu'il existe une documentation détaillée des atteintes à la protection des données dans les organisations à but lucratif, avec des efforts substantiels pour faire face à la menace, on ne peut pas en dire autant des organisations à but non lucratif en raison de plusieurs défis (Gordon et al., 2015).

Souvent, les organisations à but non lucratif manquent de financement adéquat pour développer des unités d'évaluation des TI et des contrôles qui peuvent travailler à une meilleure protection (Mierzwa et Scott, 2017). Faisant écho aux affirmations de Mierzwa et Scott, Jagalur et coll. (2018) ont constaté que les organisations à but non lucratif manquent souvent de personnel spécialisé dans la cybersécurité pour prendre en charge leur unité informatique. Selon Mierzwa et Scott, les organisations à but non lucratif manquent de budgets et de personnalités adéquats pour leurs services

informatiques, car leur objectif principal est de servir des objectifs spécifiques, de s'efforcer d'atteindre une mission et de se concentrer davantage sur l'acquisition de financement et la réduction des coûts. Selon eux, ils considèrent que les objectifs de ces organisations à but non lucratif ne s'alignent pas sur une bonne cybersécurité. Un exemple parfait qui met en évidence les arguments de Mierzwa et Scott reflète les grandes organisations caritatives telles que la Croix-Rouge. Dans de nombreux cas, la Croix-Rouge fait appel à des individus comme volontaires pour atteindre ses objectifs (International Fédération of Red Cross and Red CrescentSocieties,2019). Cependant, l'idée de travailler avec des bénévoles signifie que l'organisation peut ne pas obtenir les personnes les plus qualifiées pour servir dans leurs départements, en particulier pour des départements très exigeants comme l'informatique. Le manque de salaires compétitifs rend sans doute difficile pour les organismes sans but lucratif d'attirer les meilleures compétences informatiques, laissant la plupart d'entre eux à la merci de bénévoles moins qualifiés (Jagalur et al., 2018). Aranda et coll. (2018) ont observé que, contrairement aux travailleurs employés, les bénévoles augmentent le risque d'atteintes à la protection des données parce qu'ils ne sont peut-être pas aussi engagés envers leur contrat social que le personnel employé de façon permanente. Cependant, avec la menace toujours croissante des violations de données, les organisations à but non lucratif se sont lancées dans diverses stratégies pour se protéger contre le risque (Holtfreter &Harrington, 2015).

Stratégies à but non lucratif pour sécuriser les données

De nombreuses organisations à but non lucratif mettent en place des stratégies pour lutter contre les violations de données dans leurs locaux. Selon Bauer et coll. (2017),

l'une de ces approches consiste à sensibiliser la population aux systèmes d'information au moyen de programmes spéciaux mis en œuvre par les gestionnaires des SI. Ces programmes comprennent des interventions planifiées systématiquement qui transmettent continuellement l'information sur la sécurité au public cible (Bauer et coll., 2017). Almubark et coll. (2016) sont en tandem avec Bauer et coll., qui ont indiqué que la meilleure façon pour les organismes sans but lucratif de motiver le comportement des employés à freiner les violations de données est de créer une culture de sécurité influente. Cette stratégie fonctionne parce que la création d'une culture de sécurité influente tient les employés au courant de la technologie, notamment en leur permettant de comprendre les processus et autres facteurs organisationnels qui touchent à la sécurité des données (Almubark et al., 2016). Considérant le même argument qu'Almubark et coll., Zafar et coll. (2016) insistent sur le fait qu'une culture influente sur la sécurité des données est améliorée grâce à une formation de sensibilisation, à des activités de gestion des risques et à des activités de planification de la sécurité. Dans les organisations modernes, Zafar et coll. ont observé que le soutien de la haute direction aux pratiques de gouvernance des TI impliquait la réalisation interne d'audits de conformité, l'établissement de cadres de classification des données, l'offre d'une équipe de gouvernance des données et le poste de chef de la sécurité. Comme indiqué par Zafar et al., cet arrangement peut être reproduit dans des organisations à but non lucratif dans le but de contrôler les cas de violation de données.

En plus de sensibiliser l'organisation à la cybersécurité, l'authentification constitue également une stratégie contre les violations de données des organisations à but

non lucratif. L'authentification implique un processus permettant de vérifier l'exactitude et l'authenticité des revendications sur un sujet particulier ou concernant une question (Mohammed et coll., 2017). Dans les organisations à but non lucratif, l'instauration de l'authentification en tant que processus de sécurité des données protégerait contre tout accès non autorisé aux réseaux de l'organisation, en plus de protéger l'identité des utilisateurs et de garantir la véritable identité de l'utilisateur (Bidgoli, 2018). En particulier, Reddy et coll. (2016) ont expliqué que la plupart des protocoles cryptographiques impliquent un point de terminaison pour l'authentification cherchant à contrecarrer spécifiquement les attaques de l'homme du milieu (MITM). Une illustration parfaite de ce cadre que les organisations à but non lucratif peuvent envisager pour la sécurité de leurs données comprend le 11 Transport Layer Security (TLS) ou le Secure Sockets Layer (SSL; Liu et coll., 2018). TLS et SSL fonctionnent en chiffrant en permanence les segments de connexion réseau au niveau de la couche de transport (Liu et al., 2018). Bharathi (2017) a expliqué que les données sont le courtage, l'exposition des données personnelles à l'échelle mondiale et la déficience de la conception de la sécurité basée sur la gouvernance font partie des principaux problèmes de sécurité auxquels les organisations sont actuellement confrontées. Les organisations à but non lucratif peuvent compter sur SSL ou TLS pour vérifier le serveur via une autorité de certification de confiance conjointe (Liu et al., 2018). De plus, Pascalev (2017) mentionne la possibilité pour les organisations à but non lucratif d'utiliser l'algorithme Bull Eye pour observer toutes les informations sensibles d'un point de vue à 360 °. Lorsque les organisations à

but non lucratif utilisent cet algorithme pour leur sécurité des données, elles gèrent les relations impliquant des données répliquées et des données originales (Pascalev, 2017).

La sécurité à trois cent soixante degrés est une autre stratégie disponible pour les organismes sans but lucratif dans leurs efforts pour faire face à la menace de violation de données (Kholidy et al., 2016). La stratégie de sécurité à 360 degrés, telle que développée par Kholidy et al., est un plan visant à répondre en profondeur aux mesures de sécurité de l'organisation à but non lucratif. En accord avec Kholidy et coll., Woszczynski et Green (2017) ont constaté que la première étape de la mise en œuvre de la stratégie de sécurité à 360 degrés consistait à identifier les actifs de valeur pour s'assurer qu'ils se protégeaient des risques potentiels qui pourraient entraîner des atteintes à la protection des données. Après avoir identifié les actifs de valeur, l'objectif est de s'assurer qu'ils sont tous sous les bons contrôles (Woszczynski &Green, 2017). Cependant, il ne suffit pas de s'assurer que les actifs sont soumis aux contrôles appropriés. Moskal et coll. (2018) ont insisté sur le fait que la protection des actifs précieux par l'organisation à but non lucratif devrait être vérifiée tout au long de l'enquête au moyen de tests et de simulations appropriés. Il doit y avoir un processus existant qui guide les procédures d'amélioration et de gouvernance afin d'assurer une confiance continue dans les contrôles (Moskal et coll., 2018). Dans le même ordre d'idées, Libicki (2017b) a observé que l'organisation à but non lucratif doit disposer d'un système pratique de surveillance et d'intervention pour permettre le traitement en temps réel des événements et des atteintes présumées. Les principaux atouts précieux de la stratégie de sécurité à 360 degrés comprennent les personnes et les données / propriété intellectuelle (Libicki, 2017b). L'organisation à but

non lucratif doit protéger ces actifs vitaux en mettant en place des contrôles, des processus et de la technologie pour les protéger. Ces contrôles, procédures et technologies, selon Cobb et coll. (2018), font l'objet d'évaluations constantes afin de garantir un mécanisme de contrôle pleinement efficace.

Au cours de la mise en œuvre de la stratégie de sécurité à 360 degrés, les tests axés sur le renseignement sont essentiels (Kholidy et coll., 2016). Les organisations à but non lucratif doivent simuler toutes les formes d'attaque susceptibles d'être rencontrées et vérifier si leurs actifs sont protégés de manière adéquate. Selon Young et Drees (2018), les tests de nouvelle génération devraient être dirigés par les attaques existantes et les vecteurs de menace que les utilisateurs malveillants et autres pirates externes utilisent. Après les tests axés sur le renseignement, les organisations à but non lucratif doivent s'assurer d'améliorer la gouvernance de la sécurité (Catota et al., 2018). Catota et coll. ont affirmé que les organisations à but non lucratif doivent continuellement examiner, améliorer et évaluer leurs environnements en gérant les risques, en effectuant des audits et en s'assurant que les contrôles et les mécanismes de test mis en place protègent les actifs de grande valeur. Les résultats de ces études sont essentiels à mon étude, car l'adoption d'une approche complète et approfondie de la lutte contre les cyberattaques permet aux organisations à but non lucratif d'améliorer leur capacité à répondre à toute forme d'attaque malveillante. La stratégie de sécurité à 360 degrés crée une culture organisationnelle dans laquelle les organisations à but non lucratif défendent de manière proactive leurs ressources de données et leurs opérations contre les attaques plutôt que de rester réactives à la menace.

De plus, Bordoff et al. (2017) ont souligné la nécessité pour les organismes sans but lucratif de former leur personnel sur les meilleures pratiques en matière de sécurité et de justifier les tiers. Le prochain plan d'action pour la stratégie de sécurité à 360 degrés consiste à surveiller l'intervention en cas d'incident (Kholidy et coll., 2016). Comme le soulignent Kholidy et coll., il s'agit d'une intervention essentielle, car les rapports d'atteinte à la protection des données indiquent que de nombreux incidents d'atteinte à la protection des données demeurent inaperçus, parfois même pendant plus de six mois. Cette période prolongée allant jusqu'à six mois et au-delà des atteintes à la protection des données inaperçues implique que les pirates informatiques pourraient avoir toute la liberté d'accéder aux données qu'ils veulent de leurs victimes (Kholidy et al., 2016). En réponse aux observations de Kholidy et coll., Garlinec et coll. (2017) ont observé qu'une surveillance proactive est essentielle si les organismes à but non lucratif doivent alimenter des plans bien élaborés visant à intervenir en cas d'incident. L'élaboration de ces plans doit tenir compte du fait que la formation, la simulation et la rétroaction mènent toutes à une intervention efficace chaque fois que nécessaire (Garlinec et coll., 2017). Au cours d'un test de pénétration, le testeur peut finir par compromettre un serveur, accédant par la suite à des données sensibles ou à des privilèges élevés dans le but d'obtenir un accès à l'échelle du système à la main-d'œuvre qui le sait (Bertoglio et Zorzo, 2017). Pour cette raison, le personnel doit être sensibilisé à la façon de gérer un tel événement.

Les organismes sans but lucratif pourraient également recourir à l'informatique en nuage comme stratégie pour améliorer la cybersécurité (Hubbard et al., 2019). À cet égard, l'informatique en nuage implique les technologies qui s'appuient sur Internet

comme un podium pour garantir aux utilisateurs un accès pratiquement omniprésent à des ressources informatiques extrêmement évolutives, souples et robustes à l'aide de services en ligne hébergés dans des centres de données situés hors site (Bidgoli, 2018). Selon Nieuwenhuis et al. (2018), à l'heure actuelle, les entreprises de différentes tailles déplacent leurs systèmes informatiques « vers le cloud » afin de réaliser des opérations efficaces et efficientes. Outre l'efficacité des opérations, Wright et coll. (2017) ont noté que les organisations à but non lucratif peuvent considérer l'infonuagique comme une stratégie pour améliorer la cybersécurité et atteindre les objectifs en matière de protection de la vie privée. Comme déjà souligné, la plupart des organisations à but non lucratif ont tendance à fonctionner avec un budget serré qui finit par imposer des ressources limitées à la gestion de la cybersécurité (Jalali &Kaiser, 2018). Cependant, selon Wright et al., l'informatique en nuage peut jouer un rôle important en aidant les organismes sans but lucratif à payer pour les ressources informatiques dont ils ont besoin en fonction des besoins, économisant ainsi de l'argent. Rathi et Given (2017) étaient d'accord avec l'observation de Wright et coll., notant que l'infonuagique héberge des applications et des services situés dans des centres de données hors site gérés par un fournisseur de services infonuagistes expert. L'emplacement hors site des centres de données réduit le lourd fardeau qui serait autrement dû aux organismes à but non lucratif alors qu'ils cherchent à installer, mettre à jour régulièrement et maintenir le matériel et les logiciels (Rathi & Given, 2017).

Le rôle le plus crucial de l'informatique en nuage est de présenter une alternative immédiate pour garantir la sécurité des données pour les organismes à but non lucratif

sans nécessiter d'investissement initial substantiel (Attaran, 2017). La sécurité des données est importante pour la cybersécurité ainsi que pour l'exécution de la protection des données. L'exigence essentielle de lois complètes sur la sécurité des données, telles que le règlement général sur la protection des données et la directive sur la protection des données, exige que les organisations traitant des données personnelles forment leur personnel sur les mesures techniques et organisationnelles nécessaires en matière de sécurité (Dove, 2018). Ces mesures garantissent la protection de toutes les données personnelles qu'ils stockent ou traitent (Malgieri & Comandé, 2017). Le respect de ces exigences peut ne pas être possible à moins qu'une organisation à but non lucratif ne mette en œuvre des systèmes et des mesures de protection adéquats qui empêchent la divulgation ou l'accès malveillant à ses données. Cependant, les organismes sans but lucratif ont du mal à se conformer à ces exigences générales en raison de leurs ressources limitées et de leurs compétences techniques pour appliquer des systèmes de sécurité locaux complets (Wright et al., 2017). Dans ces cas, Rathi et Given ont noté que les solutions cloud servent à offrir un coup de pouce significatif à la sécurité des données à but non lucratif sans nécessairement exiger des compétences techniques plus élevées, un investissement en temps et un coût.

Les systèmes cloud garantissent une plus grande sécurité, en particulier pour les organisations à but non lucratif mal financées, car certaines des entreprises de sécurité nécessaires des systèmes cloud incluent le chiffrement de bout en bout (Baseri et al., 2018). Le chiffrement couvre à la fois les données stockées en interne et les données en transit entre l'organisation cliente et le centre de données cloud. De plus, Kajiyama et

coll. (2017) ont noté que les systèmes infonuagiques offrent une sécurité physique de pointe qui comprend un examen minutieux 24 heures sur 24, des contrôles d'accès physiques, ainsi qu'une protection périmétrique à plusieurs niveaux. Rossouw et Willett (2017) ont noté que les systèmes infonuagiques sont tenus de se conformer aux normes de protection des données, telles que ISO 27002, ISO 27017 et ISO 27018, en plus de se conformer à la sécurité internationale. Ces fonctionnalités garantissent une grande partie de l'infrastructure de cybersécurité robuste, dont une grande partie de nombreuses organisations à but non lucratif peuvent se permettre d'établir dans le cadre de leur infrastructure sur site (Rossouw &Willett, 2017).

Gouvernance des données

La gouvernance des données fait référence à un cadre à l'échelle de l'entreprise visant à attribuer des droits et des devoirs liés à la décision dans le but de traiter adéquatement les données en tant qu'actif de l'entreprise (Alhassan et al., 2016). Essentiellement, l'objectif principal de la gouvernance des données est de faire des données un élément essentiel de l'entreprise (Alhassan et coll., 2016). Pour les organismes sans but lucratif comme les églises et les hôpitaux, leurs volumes de données ont explosé après des années d'opérations continues dans leurs domaines de compétence (Lee, 2016). La gouvernance des données est essentielle à la cybersécurité car elle augmente de nombreuses lignes de protection pour les données à risque (Yang et al., 2019). Selon Yang et coll., les données à risque impliquaient des données qui compromettraient l'organisation si elles devaient être consultées par des personnes non autorisées. L'identification de ce type de données est cruciale, en gardant à l'esprit qu'il

est impossible de sécuriser toutes les données pour la plupart des organisations (Sarabi et al., 2016). L'émergence continue de technologies visant à aider les organismes sans but lucratif à gérer efficacement leur charge accrue peut ne pas être adéquate. Les organismes sans but lucratif peuvent ne pas être au courant des données existantes, de l'endroit où elles se trouvent ou de la façon dont les diverses unités de l'organisation et d'autres entités tierces les utilisent (Pearce, 2017). Par conséquent, sur la base de ces aspects, Pearce a justifié l'importance de la gouvernance des données en raison de son équipement vers la maximisation de l'efficacité opérationnelle en garantissant la valeur des données, en améliorant la prise de décision et en appliquant la conformité réglementaire. En accord avec Pearce, Rainie et coll. (2017) ont affirmé que la gouvernance des données aide également les organismes sans but lucratif dans leur quête pour minimiser les faibles risques de gestion des données. De nombreuses organisations à but non lucratif, en particulier celles bien établies, telles que la Croix-Rouge, disposent déjà d'une base de gouvernance des données supérieure. Cependant, ils revoient rarement leur stratégie, même s'ils intègrent de nouvelles plateformes de données et d'analyse (Rainie et coll., 2017). Il existe plusieurs activités ou piliers de gouvernance des données que les organisations à but non lucratif peuvent prendre en compte pour leur sécurité.

La première pratique de gouvernance des données est axée sur les processus, les politiques, les normes et les procédures (Rainie et coll., 2017). Selon Rainie et al., la gouvernance des données de l'organisation à but non lucratif, tout comme dans d'autres organisations, doit refléter l'orientation stratégique de l'entreprise et les résultats souhaités en matière de gestion des données, de sécurité de l'information, d'architecture

et de modélisation des données. Yeong et Suh (2018) sont d'avis que les organisations telles que les organismes à but non lucratif doivent tenir compte de l'évolution des processus, des normes, des politiques et des procédures dans leurs efforts pour poursuivre une gouvernance efficace des données. En particulier, Yeong et Suh ont fait valoir que les organisations à but non lucratif qui mettent en œuvre de nouvelles plateformes de données doivent, tout d'abord, envisager l'automatisation des processus. Les plates-formes plus récentes avec une puissance de traitement pour de grands volumes de données peuvent rendre possible des analyses plus interactives, expérimentales et évolutives (Yeong &Suh, 2018). Lorsque les organisations à but non lucratif finissent par atteindre leur échelle améliorée et traitent directement des informations complexes, elles améliorent finalement leur potentiel à entreprendre des opérations de gestion des données (Kuerbis &Badiei, 2017). Selon Kuerbis et Badiei, de nombreux processus, tels que les validations de la qualité des données ou la découverte de métadonnées, peuvent être améliorés en raison de l'automatisation au moyen de technologies cognitives.

Les pratiques de gouvernance des données doivent être également démocratisées si, du tout, les organismes sans but lucratif ont l'intention d'obtenir des résultats positifs (Parks et al., 2017). Dans les organismes sans but lucratif, l'échelle et la complexité des données augmentent toujours et, par conséquent, cela oblige la responsabilité de la gestion des données à changer de propriétaire (Park et al., 2016). À ce titre, Park et coll. ont soutenu qu'il est essentiel que la direction des organismes sans but lucratif dote l'organisation des outils, normes, processus et procédures de collaboration nécessaires pour garantir une gestion efficace. Enfin, en mettant l'accent sur les opérations, les

politiques, les procédures et les normes, il est toujours essentiel pour la direction des organismes sans but lucratif d'apprécier que les normes et les procédures évoluent continuellement pour ouvrir la voie à de nouveaux prototypes architecturaux (Williams &Woodward, 2015). Faisant écho à Williams et Woodward, Prakash et Singaravel (2015) ont ajouté que les organismes à but non lucratif opéraient continuellement dans un environnement où leurs paysages analytiques et opérationnels ne cessaient de changer. Les organisations à but non lucratif doivent stocker des copies des données qu'elles traitent dans des emplacements physiques distincts, ce qui rend la gestion plus difficile et prédisposée aux compromissions de sécurité. Pour cette raison, on s'attend donc à ce que les organismes sans but lucratif progressent leurs procédures et leurs normes à des fins de sécurité et d'architecture des données (Prakash &Singaravel, 2015).

La deuxième pratique de gouvernance des données est axée sur les organisations, les rôles et les responsabilités(Garlinec et coll., 2017). Ces auteurs affirment que de nombreux organismes à but non lucratif ont mis au point des arrangements de gouvernance des données qui englobent des tâches et des rôles bien définis pour faciliter et superviser les processus de gestion des données. Cependant, Burns et coll. (2017) avaient un point de vue différent de celui de Garlinec et coll., notant que de nouvelles plateformes émergent et que les chances que les organisations, les responsabilités et les rôles changent également. Ainsi, les organismes sans but lucratif doivent mettre en place plusieurs considérations. Ils doivent envisager d'étendre la gouvernance des données au développement (Burns et coll., 2017). Une plus grande gouvernance sera nécessaire en rendant compte des données au-delà de la sphère primaire de la gestion des données

jusqu'au développement du cycle de vie des logiciels (Kuerbis &Badiei, 2017). À ce titre, Anand et coll. (2018) ont exposé les affirmations de Kuerbis et Badiei, notant que cela mènerait à un processus plus proactif de gouvernance des données.

D'autre part, la gouvernance des données réduirait la nécessité de résoudre les problèmes de plate-forme de production. En plus d'étendre la gouvernance des données au développement, il est également nécessaire pour les organisations à but non lucratif d'avoir des gestionnaires de perfectionnement dans leurs efforts de gouvernance des données (Anand et al., 2018). Ces intendants apporteront une crédibilité technique pour s'adapter aux modifications technologiques émergentes telles que les mégadonnées, les plateformes compatibles avec le cloud, les microservices et les données en continu (Anand et al., 2018). Selon Anand et al., les organisations à but non lucratif peuvent offrir une formation qui aiderait les intendants à s'acquitter efficacement de leurs fonctions sur les plateformes de données modernes. Enfin, la prise en compte nécessite une orientation sur les fonctions de sécurité des données(DiMase et coll., 2015). Faisant écho à DiMase et coll., Stewart et Jürjens (2017) ont observé que l'utilisation de plusieurs canaux pour accéder à l'information à la fois à l'intérieur et à l'extérieur de l'entreprise augmente les niveaux de risque pour la sécurité des données. Principalement, les organisations à but non lucratif doivent également introduire des technologies perturbatrices dans leur tentative de contrôler l'utilisation et l'accès aux données (Stewart &Jürjens, 2017). En examinant ces nombreuses études, j'ai établi des informations riches qui ont aidé à développer des stratégies de sécurité informatique pratiques que les organisations à but non lucratif utilisaient pour protéger les informations contre les cyberattaques.

Sécurité et confidentialité

Dans une organisation à but non lucratif, la protection de la vie privée est décrite comme la capacité de protéger des renseignements sensibles (Martin et Murphy, 2017). Pour les organismes sans but lucratif tels que les hôpitaux, la protection de la vie privée implique la protection des informations de soins de santé personnellement identifiables à leur disposition(Abouelmehdi et al., 2017). Selon Adams (2017), les organismes sans but lucratif n'ont protégé les renseignements personnels qu'après l'enracinement des processus de stockage et de transport dans les mesures de sécurité. Adams a notamment suggéré une série de mesures que les organisations à but non lucratif peuvent envisager dans leur quête pour maintenir la sécurité et les privilèges pour se prémunir contre les violations de données.

Premièrement, les organismes sans but lucratif devraient envisager des moyens systématiques et efficaces d'éliminer les renseignements personnels qu'ils détiennent, en particulier lorsque ces renseignements ne sont plus nécessaires sous leurs formes simples (Adams, 2017). Les explications de Maras (2015) semblent être en tandem avec celles d'Adams, notant que la quantité absolue de données échangées dans une organisation à but non lucratif augmente de manière exponentielle. La croissance exponentielle crée un risque sur la sécurité des données car, selon Maras, même les systèmes très dynamiques peuvent ne pas sécuriser la confidentialité de ces informations, en particulier avec le risque de diffusion de données à partir de nouveaux objets et appareils. Samani et coll. (2015) ont suggéré que les organisations telles que les organismes à but non lucratif peuvent réduire le risque que leurs nouveaux serveurs soient ciblés par des pirates en

maintenant simplement la diligence dans le respect des procédures de rejet des données. Dans l'environnement actuel de l'Internet des objets (IdO), les organismes sans but lucratif peuvent être plus à risque de laisser leur vie privée exposée si leurs pratiques de traitement et de gestion des données restent incohérentes (Samani et coll., 2015).

Deuxièmement, les organismes sans but lucratif doivent également être conscients que les domaines public-privé des politiques et des protections deviennent parfois flous en ce qui concerne le contexte d'échange de données (van de Pas &van Bussel, 2015). Ce flou signifie que les politiques des institutions publiques visant à limiter la collecte de données peuvent ne pas exister dans les organisations à but non lucratif. Par exemple, les personnes au sein de la société peuvent ne pas choisir de divulguer leurs renseignements personnels à des organismes sans but lucratif; cependant, une telle divulgation augmente le risque d'exposer les informations privées des individus à des pirates informatiques et à des violations de données.

Troisièmement, les organismes sans but lucratif doivent explorer l'approche de dépersonnalisation comme moyen de protéger leur sécurité et leur vie privée contre les atteintes à la protection des données (Quirós et coll., 2015). La désidentification fait référence à une technique traditionnelle qui consiste à interdire la divulgation de renseignements confidentiels en refusant tout détail pouvant reconnaître une personne (Abouelmehdi et coll., 2017). La technique de dépersonnalisation, selon Abouelmehdi et al., fonctionne en supprimant des identifiants particuliers des données. Cependant, même avec ces mesures, Kayaalp (2018) a fait valoir que les attaquants peuvent toujours accéder à une aide supplémentaire en matière d'informations externes pour la

dépersonnalisation. En particulier, les attaquants ciblent des organisations à but non lucratif telles que les hôpitaux où le Big Data est impliqué. Soulignant son point, Kayaalp a donc insisté sur le fait que la dépersonnalisation n'est pas une approche suffisante par laquelle les organisations à but non lucratif peuvent protéger la confidentialité des données critiques. Au lieu de cela, Kayaalp a suggéré la nécessité pour les organisations à but non lucratif de trouver des algorithmes efficaces de préservation de la vie privée comme moyen d'atténuer le risque de réidentification. Rajendran et coll. (2017) ont mentionné les concepts d'anonymat k, de diversité l et de proximité t que des organisations comme les organismes à but non lucratif peuvent avoir besoin de prendre en compte pour améliorer cette technique traditionnelle. La technique de l'anonymat k fonctionne de sorte qu'à mesure que la valeur de k augmente, la probabilité de réidentification diminue (Rajendran et coll., 2017). Néanmoins, Quirós et coll. (2015) ont souligné que cette technique peut produire des distorsions de données dans l'organisation, entraînant une perte d'information plus importante. En outre, Quirós et al. ont expliqué qu'une anonymisation excessive risque de rendre les données divulguées moins utiles, en particulier pour les destinataires, car certaines analyses peuvent finir par fournir des résultats erronés et biaisés.

Quatrièmement, les organismes à but non lucratif doivent réévaluer leurs processus et politiques en matière de protection de la vie privée en mobilisant tous leurs intervenants (Pouloudi et coll., 2016). Pour les organismes sans but lucratif comme les hôpitaux, l'engagement des parties prenantes devrait inclure les infirmières, les médecins, les compagnies d'assurance, les administrateurs et tous les autres associés commerciaux

(Pouloudi et coll., 2016). Expliquant la logique qui sous-tend ce raisonnement, Parks et coll. (2017) ont mentionné que lorsque des intervenants provenant de divers domaines participent à la pratique de l'organisation en matière de protection de la vie privée, la probabilité de conséquences négatives est limitée. Selon Parks et al., de simples politiques de confidentialité seulement peuvent s'avérer pratiquement dénuées de sens et très superficielles pour une organisation à but non lucratif à moins que les parties prenantes ne s'impliquent dans le développement, la surveillance et l'application de la même chose. D'accord avec Parks et coll., Lim et coll. (2018) ont ajouté que les organismes sans but lucratif ont besoin d'une véritable protection de la vie privée et d'une véritable défense des droits dans le cadre du processus de formation de l'organisation.

De plus, Lim et coll. (2018) ont indiqué que les organisations comme les organismes sans but lucratif doivent permettre à la haute direction d'être à l'avant-garde en ce qui concerne la protection et la défense réelles de la vie privée. Les dirigeants d'un organisme à but non lucratif comme un hôpital doivent comprendre l'importance de minimiser les conséquences imprévues s'ils cherchent à réduire le problème de déséquilibre (Abouelmehdi et coll., 2018). En général, ces mesures aident à déterminer les détails critiques qui établiraient efficacement des stratégies de sécurité informatique pratiques contre les cyberattaques contre les organisations à but non lucratif, soutenant ainsi ma question de recherche.

Rôles de travail associés aux responsables de la sécurité des systèmes d'information

Le rôle des responsables de la sécurité de l'information est au centre de beaucoup d'attention ces dernières années. Les ISSM jouent des positions influentes dans la lutte contre les cybermenaces, l'application des politiques de sécurité et la gestion des employés. Selon Al-Taie et coll. (2018), le DPI assume six rôles importants : élaborer des stratégies pour l'innovation et la refonte des processus d'affaires basés sur les TI, servir d'architecte des relations avec des fournisseurs de services informatiques remarquables et intégrer le traitement, l'information et l'aide à la décision. Les autres rôles du DPI comprennent l'éducation de la haute direction sur la TI et sa valeur pour l'organisation, la prestation de services publics de services d'infrastructure de TI et le rôle de gestionnaire de l'information de l'organisation pour des systèmes fiables sur le plan opérationnel et des données de haute qualité (Al-Taie et coll., 2018). Tumbas et coll. (2018) résument le rôle du DPI en tant que domaine institutionnalisé chargé de détenir la compétence en matière d'innovation avec les technologies numériques. En règle générale, Tumbas et al. ont caractérisé le comportement du DSI comme structuré selon les normes professionnelles informatiques, y compris l'intégration de systèmes et la maximisation des tâches commerciales constantes.

Le RSSI assume le rôle d'aider à maintenir la relation client et d'accroître la rétention en protégeant la réputation de l'entreprise et les informations confidentielles sur les clients (Lanz, 2017). De plus, Lanz a déclaré que le RSSI élabore et surveille la conformité aux procédures et aux politiques de cybersécurité et surveille et évalue ses activités techniques pour gérer les risques liés à la technologie en conséquence. Les

autres rôles des RSSI incluent la conformité aux réglementations liées à la technologie, la préparation de tests et de rapports concernant la résilience de l'entreprise et la gestion de la supervision à l'échelle de l'organisation des fournisseurs de services tiers. Les RSSI mènent également des enquêtes de gestion sur l'utilisation générale de la technologie dans l'organisation et servent de contact principal au sujet de l'application de la loi (Lanz, 2017).

Transition et résumé

Dans la section 1, j'ai couvert l'introduction, décrivant les informations de base de l'étude. J'ai inclus 12 éléments principaux dans la section qui couvraient largement le fondement et la portée de l'étude. Les domaines de cette section comprenaient le contexte du problème, l'énoncé du problème, l'énoncé de l'objectif, la nature de l'étude, les questions de recherche, le cadre conceptuel, les termes opérationnels, les hypothèses, les limites de la recherche, les délimitations, l'importance de l'étude et, enfin, un résumé des travaux professionnels et savants de la littérature examinée.

Dans la section 2 de l'étude de recherche, j'ai couvert les participants à l'étude et la méthode de recherche, la conception, l'échantillonnage de la population, l'éthique de la recherche, les instruments de collecte de données, les techniques de collecte de données, l'analyse des données, ainsi que la fiabilité et la validité. J'ai également couvert des détails détaillés sur la méthodologie et le processus de recherche à adopter. Dans la section 3, j'ai présenté les constatations, appliqué les constatations à la pratique professionnelle, couvert les répercussions sur le changement social, formulé des

recommandations d’action, formulé des recommandations pour une étude plus approfondie, offert des réflexions et, enfin, résumé et inclus la conclusion de l’étude.

Section 2 : Le projet

Dans cette étude, j'ai cherché à explorer les stratégies de cyberattaque pour les organisations à but non lucratif. La section 2 de ce projet illustre des détails détaillés sur la méthodologie et le processus de recherche que j'ai adoptés. Dans l'ensemble, cette section comprend l'énoncé de l'objectif, le rôle du chercheur, des détails sur les participants, la méthode et la conception de la recherche, ainsi que la population de recherche. D'autres sujets comprennent la méthode d'échantillonnage, la collecte de données, l'organisation et l'analyse, ainsi qu'une réflexion sur la fiabilité et la validité.

Énoncé de l'objet

L'objectif de cette étude de cas qualitative multiple était d'explorer les stratégies que les ISSM des organisations à but non lucratif utilisaient pour se protéger contre les cyberattaques. La population spécifique comprenait des responsables informatiques et des directeurs informatiques en charge de la gestion de la sécurité dans des organisations à but non lucratif du Maryland, du district de Columbia et de Virginie. J'ai mené l'étude à différents endroits en utilisant les informations des participants. Les implications de cette étude en matière de changement social sont que les personnes responsables ou engagées avec des organisations à but non lucratif pourraient réduire le vol d'identité et améliorer les environnements sûrs. L'impact du changement social pourrait être considérable parce que les victimes de cyberattaques subissent des pertes financières, des perturbations opérationnelles, des dommages à la réputation et des ramifications juridiques, entre autres effets néfastes. Avec la nature omniprésente des cyberattaques, de nombreuses personnes ont souffert de données volées et mal utilisées.

Rôle du chercheur

La pratique de la recherche qualitative exige que le chercheur assume le rôle de l'instrument dans la collecte de données primaires (Daniel, 2018). J'ai été le principal instrument de collecte de données dans mon étude. Essentiellement, les chercheurs qualitatifs doivent se développer a) pour devenir des instruments de recherche permettant de recueillir des données auprès de la population de l'échantillon de recherche; b) concevoir, interpréter et entreprendre une analyse qualitative des données; et c) présenter les résultats de l'étude tout en tenant compte des normes éthiques et de haute qualité (Marshall et Rossman, 2016).

L'expérience personnelle d'un chercheur influence les études qu'il mène (Thistoll et coll., 2016). Je me considérais comme le chercheur expérimenté dans cette étude en ce que j'ai étudié l'informatique à des niveaux d'éducation plus élevés. J'ai une bonne compréhension de la sécurité et de la gestion des données et une bonne connaissance de certaines des stratégies utilisées pour les organisations de sécurité des données. Je me suis concentré sur l'atténuation des effets de mes expériences en tant que chercheur dans le cadre de mon étude afin d'éviter les préjugés. J'ai vécu à Frederick, dans le Maryland, et j'ai travaillé dans l'informatique. Je n'avais aucune relation professionnelle avec les participants à l'étude. Ces facteurs auraient pu apaiser les inquiétudes des participants concernant la divulgation de détails sensibles ou apaiser leur réticence à participer à l'étude.

Les préjugés avaient le potentiel d'influencer mon étude. Les pratiques visant à atténuer les biais dans la recherche qualitative comprennent l'utilisation de plusieurs

personnes interrogées, la triangulation des données, la mise en œuvre de la vérification des membres et le respect d'un protocole d'entrevue (Ranney et coll., 2015). J'ai utilisé des données obtenues des personnes interrogées ainsi que des documents organisationnels pour effectuer une triangulation méthodologique.

J'ai mené les entrevues pour offrir aux participants l'occasion d'expliquer librement les problèmes et les incidents de cybersécurité dans leur organisation. L'adoption du protocole d'entrevue m'a aidé à avoir une compréhension critique du sujet de recherche. Selon Henry et Foss (2015), les protocoles d'entrevue sont essentiels lors de l'utilisation de la méthode d'entrevue, car ils offrent au chercheur des conseils pour recueillir des données fiables.

En tant que chercheur dans cette étude, j'ai suivi le protocole d'entrevue (annexe) pour garantir que j'ai maintenu l'uniformité pendant le processus d'entrevue. Les chercheurs doivent respecter strictement le protocole d'entrevue pour s'assurer d'éviter la partialité de leurs résultats (Ngongo et coll., 2015). En tant que chercheur, j'étais tenu d'adhérer aux principes éthiques et aux lignes directrices stipulés dans le *rapport Belmont* (Commission nationale pour la protection des sujets humains de la recherche biomédicale et comportementale, 1979). Ces principes et orientations sont conçus pour protéger les sujets humains qui participent à la recherche, pour ne causer aucun préjudice et traiter les participants équitablement (Adashi et coll., 2018). J'ai suivi la formation des National Institutes of Health (NIH) sur la protection des participants humains à la recherche afin de mieux comprendre les défis éthiques et la protection des participants. La participation était volontaire et sans contrainte. Un protocole d'entrevue est essentiel pour aider

l'intervieweur à se préparer à l'entrevue, notamment pour s'assurer que les questions sont connues et déterminer l'information la plus essentielle à la recherche (Majid et coll., 2017).

Participants

J'ai choisi les participants à cette étude parmi les responsables informatiques et les directeurs informatiques issus de cinq organisations à but non lucratif. J'ai sélectionné des participants qui avaient de l'expérience dans la sécurité des données et la gestion des risques. Dans cette étude, les participants devaient avoir de l'expérience dans la sécurité des données et la gestion des risques et au moins 5 ans de travail dans le département informatique des organisations à but non lucratif. L'admissibilité des participants à une étude va de leur expérience et de leurs connaissances sur le sujet à l'étude (Akaeze, 2016). Les chercheurs doivent avoir des principes et des critères clairs pour guider la sélection des participants à une étude de recherche (Daniel, 2018). L'importance de ces principes clairs donne aux chercheurs la possibilité d'évaluer les résultats de la recherche et l'étendue de la transférabilité. Gaus (2017) a observé que l'utilisation par un chercheur de critères de sélection des participants aide à déterminer la crédibilité, l'identification exacte et la description des participants.

Morris et Rosenbloom (2017) ont expliqué que les chercheurs ont besoin de l'autorisation du Comité d'examen institutionnel(CISR) avant de communiquer avec les participants à leur étude. J'ai cherché sur le site Web tax-exempt world, un référentiel consultable qui est librement accessible au public et répertorie toutes les organisations à but non lucratif en Amérique. J'ai sélectionné cinq organisations à but non lucratif sur le

site Web qui répondaient à mes critères de recherche et j'ai contacté les contacts des organisations. J'ai envoyé un email aux personnes de contact identifiées sur le site. Dans la correspondance, j'ai fait part de mon intention de faire des recherches sur l'organisation, y compris le but et les objectifs. J'ai demandé aux participants potentiels de me contacter en utilisant l'adresse e-mail ci-jointe. Selon Hampton et coll. (2019), bien qu'une étude de recherche puisse compter entre quatre et quinze participants, l'objectif de toute recherche devrait toujours être de recueillir des données denses et riches. Le nombre total de participants ne devrait pas être un sujet de préoccupation, mais plutôt la richesse des données éventuelles. Une fourchette d'échantillons de trois à huit s'applique de façon appropriée dans les études de cas (Yin, 2017). Après avoir obtenu l'approbation de l'Université Walden et la correspondance de reconnaissance des participants exprimant leur volonté de participer, j'ai entrepris d'établir une relation de travail avec les participants avec l'aide des gardiens des organisations. Conformément à l'observation de Pelosi (2015), j'ai communiqué avec les participants potentiels pour établir une confiance mutuelle afin d'établir la confiance. Selon Pelosi (2015), il est essentiel de créer une communication ouverte avec les participants à la recherche, car cela donne aux parties l'assurance de la confidentialité. Pour créer une communication ouverte, j'ai a) établi un sentiment mutuel de convivialité et souligné les intérêts communs que nous partagions ; (b) décrit le sujet de recherche, mon intérêt pour l'étude, répondu aux questions des participants et veillé à ce que les participants se sentent libres et faciles; c) a rassuré les participants sur le fait que l'intégrité des données serait maintenue tout au long du processus de recherche, et d) a souligné à nouveau la

confidentialité du participant. J'ai également e) assuré une interaction positive et professionnelle en étant poli et en maintenant une attitude sans jugement; et f) écouté activement les personnes interrogées et s'est engagée avec elles pendant toute la durée des séances. Lorsque les participants à la recherche développent leur confiance dans le chercheur, ils font confiance à l'environnement de travail, ce qui renforce la crédibilité en général (Pelosi, 2015).

Méthode de recherche et conception

Méthode

J'ai choisi la méthode qualitative à utiliser dans cette étude. La méthode de recherche qualitative était idéale pour cette étude parce que cette méthodologie convient à la recherche visant à explorer et à comprendre le sens que les individus ou les groupes accordent aux problèmes humains ou sociaux. La recherche qualitative est exploratoire et sert à comprendre le comportement humain, les groupes, les phénomènes et les individus (Cavalcanti, 2017). Les chercheurs exploratoires utilisent des approches interprétatives pour la collecte, l'analyse et l'interprétation des données de recherche. L'objectif de la recherche exploratoire est de déterminer les réponses aux questions *comment* et *pourquoi* d'un phénomène. L'analyse exploratoire ne s'occupe pas du *quoi, du où* et *du quand* d'un phénomène (Gaus, 2017). Les études qualitatives aboutissent souvent à des résultats tangibles en utilisant des pratiques bien documentées d'assemblage et d'analyse de données (Shukla, 2016).

Contrairement à la méthode de recherche qualitative, la méthode de recherche quantitative repose sur des données statistiques pour tirer des résultats après l'analyse

(Hammarberg et coll., 2016). Selon Cerniglia et coll. (2016), les prémisses de la recherche quantitative comprennent la probabilité et les statistiques. Dans mon étude, l'objectif n'impliquait aucune hypothèse de mise à l'essai ou de recherche de données statistiques. La plupart du temps, je n'ai pas choisi de méthode de recherche quantitative parce que je ne prévoyais ni de tester d'hypothèses ni d'analyser des données statistiques.

L'approche fondée sur les méthodes mixtes met l'accent sur la combinaison, le rassemblement, l'amélioration et la démonstration des résultats de la recherche à l'aide de méthodes quantitatives et qualitatives (Wardale et coll., 2015). L'approche combinée rend la recherche sur les méthodes mixtes plus utile lorsqu'il s'agit de concevoir, de construire et de tester des théories, en plus de compléter l'analyse inductive et déductive dans des études centrées sur une question de recherche centrale et des hypothèses (Wardale et al., 2015). Cameron et coll. (2015) ont établi que la recherche à méthodes mixtes donne aux chercheurs la possibilité de joindre les expériences des participants et les données empiriques pour permettre de déterminer les relations existantes entre des variables particulières. Parce que je cherchais spécifiquement les idées des participants à mon étude, le choix de la recherche sur les méthodes mixtes, qui se concentre davantage sur l'examen des expériences combinées, des relations et des hypothèses entre les variables, n'était pas idéal. Je n'ai pas choisi l'étude des méthodes mixtes pour cette recherche.

Conception de la recherche

Pour cette recherche, j'ai adopté la conception qualitative d'études de cas multiples comme le choix approprié pour explorer les stratégies que les organisations à

but non lucratif utilisaient pour se protéger contre les cyberattaques. Conceptions de recherche qualitative existent dans différents types, y compris l'ethnographie, étude de cas, et la phénoménologie (Mohajan, 2018). Ces approches comportent des caractéristiques de recherche similaires concernant le problème de recherche, les données, l'analyse des données, les questions et les résultats de la communication. Le type de conception ethnographique de l'enquête qualitative s'applique principalement à l'étude des personnes et des cultures. L'application de l'ethnographie dans la recherche nécessite d'observer les participants à l'étude tout en dans leurs habitats naturels pour comprendre profondément leurs expériences, perceptions, création, et la navigation du monde social (Wels, 2015). Le chercheur recueille les données dans un contexte riche à partir de nombreuses sources de preuves dans une situation réelle (Dasgupta, 2015). Je n'ai pas choisi la conception de la recherche ethnographique parce que l'étude n'a pas impliqué des observations de culture de groupe. Le plan de phénoménologie examine la signification des occurrences vécues qu'une ou plusieurs personnes, en tant que groupe, ont collectivement vécues (Mohajan, 2018) et aide également le chercheur à séparer les biais et les hypothèses (Larkin et coll., 2019). Je n'ai pas tenu compte de la conception phénoménologique de cette recherche parce que le but ne ciblait pas les expériences vécues par les participants.

La conception de l'étude de cas se concentre principalement sur l'exploration des systèmes bornés au fil du temps (Corti et Fielding, 2016). L'exploration des systèmes bornés se déroule dans le cadre d'un exercice de collecte de données élaboré et approfondi. Les études de cas sont les plus utiles pour leur souplesse lorsqu'elles sont

utilisées parallèlement aux méthodes de recherche qualitative (Morgan et coll., 2017). Selon Corti et Fielding (2016), la conception de l'étude de cas permet à un chercheur d'obtenir une compréhension plus exhaustive d'une question donnée dans un délai précis. Parce que j'avais l'intention d'utiliser une plus grande flexibilité dans ma quête pour en savoir plus sur certaines des stratégies que les ISSM dans les organisations à but non lucratif emploient pour se protéger contre les cyberattaques dans les organisations à but non lucratif, j'ai choisi d'adopter la conception de l'étude de cas. La conception qualitative de l'étude de cas a intégré ma vision pragmatique du monde, le cadre conceptuel de la TPS, une petite taille d'échantillon, les méthodes de collecte de données, l'analyse et les contraintes de temps limitant la réalisation d'une étude doctorale dans un délai donné.

Selon Saunders et coll. (2018), un chercheur rencontre la saturation des données lorsque les entrevues qui en résultent avec des participants à la recherche ne donnent pas lieu à de nouveaux thèmes. Les chercheurs qualitatifs peuvent éviter une telle situation en interrogeant plus de participants jusqu'à ce qu'ils atteignent la saturation des données (Elman et coll., 2016). Boddy (2016) a noté que les chercheurs qualitatifs peuvent cesser d'interviewer d'autres participants à l'étude lorsque d'autres entrevues ne fournissent aucun nouveau détail concernant le sujet de recherche. Dans cette recherche, j'ai recruté des participants et recueilli des données auprès d'eux jusqu'à ce que je ne puisse pas établir l'émergence de nouveaux thèmes sur les stratégies que les ISSM dans les organisations à but non lucratif emploient pour se protéger contre les cyberattaques dans les organisations à but non lucratif.

Population et échantillonnage

Les experts en recherche conseillent le nombre idéal de participants qui devraient être impliqués dans un échantillon. Boddy (2016) a observé que la recherche qualitative ne comportait pas de règles précises sur la taille de l'échantillon. Boddy a également cité une autre étude de Sandelowsky (1995), dont les résultats ont observé que la taille des échantillons de 50 est importante pour les travaux de recherche qualitative. Les recommandations d'autres chercheurs permettent différentes tailles d'échantillonnage selon les critères de recherche (Williams et Needham, 2016). Dans cette étude, j'ai choisi les participants parmi les ISSM tirés de cinq organisations à but non lucratif librement accessibles au public dans le Maryland, le district de Columbia et la Virginie. Chaque organisme à but non lucratif est un cas unique dans une étude de cas multiple. Je croyais que les entrevues et les documents publiés et non publiés par les organisations produiraient suffisamment de données pour la triangulation.

Il existe deux techniques d'échantillonnage : la probabilité et la non-probabilité (Lucas, 2016). Une technique d'échantillonnage téléologique est une méthode d'échantillonnage non probabiliste qui donne au chercheur la liberté de choisir des participants qualifiés pour éclairer la question de recherche (Benoot et coll., 2016). Selon Hennink et coll. (2017), une technique d'échantillonnage téléologique facilite la sélection intentionnelle des participants en utilisant des caractéristiques individuelles uniques concernant le sujet à l'étude. Ridder (2017) a soutenu que l'utilisation de l'échantillonnage téléologique cadre de façon appropriée à la recherche sur les études de

cas, car elle permet de déterminer les participants qui seront utiles pour répondre à la question de recherche.

Eriksson (2017) a identifié l'échantillonnage téléologique comme étant important, en particulier lorsqu'il s'agit de groupes homogènes de participants, car il améliore l'activité d'exploitation de toute étude de recherche. J'ai choisi l'échantillonnage téléologique homogène pour cette recherche parce qu'il a amélioré l'activité d'exploitation pendant l'étude de recherche. Les participants à la recherche avaient des caractéristiques communes d'être des ISSM avec une expérience dans la sécurité des données et la gestion des risques, et avec une expérience d'au moins cinq ans de travail dans le département informatique des organisations à but non lucratif.

L'utilisation de la saturation des données dans la recherche constitue un principe directeur pour tester la suffisance de l'échantillonnage téléologique (Hennink et coll., 2017). Selon Constantinou et coll. (2017), la saturation des données survient une fois que les données deviennent redondantes ou commencent à se répliquer. Les chercheurs se lancent dans un processus précis de saturation des données pour s'assurer qu'il n'y a pas de négliger différentes significations, de nouvelles données, de nouveaux problèmes ou de nouveaux codages qui surgit. J'ai fait de la saturation des données mon objectif principal. Je n'ai pas arrêté la collecte de données jusqu'à ce que je remarque que les participants commencent à dupliquer l'information ou que l'information offerte n'a pas de valeur pour le sujet de recherche.

La collecte de données a été menée virtuellement pour éviter les interactions sociales et prévenir la propagation du coronavirus comme alternative à un bureau privé.

J’ai utilisé les stratégies de sécurité informatique des organismes à but non lucratif contre les cyberattaques Questions (voir l’annexe) pour enquêter sur les points de vue et les idées des participants concernant les pratiques de cybersécurité dans leurs organisations. Lorsque le cadre de l’entrevue est détendu, les participants seront encouragés à poser des questions et à y répondre librement (Qu &Dumay, 2011).

Recherche éthique

Après avoir obtenu l’approbation de poursuivre la recherche Walden IRB(approbation n ° 09-18-20-0682479),j’ai sélectionné les organisations à but non lucratif ciblées à participer à l’étude. J’ai envoyé par courriel un formulaire de consentement éclairé, demandant à ceux qui répondent aux critères d’admissibilité de remplir le formulaire pour vérifier leur volonté de participer à l’étude. Les renseignements essentiels inclus définissaient le but de l’étude, le rôle du chercheur, les critères de participation et le processus de retrait dans le formulaire de consentement. Parmi les autres détails du formulaire de consentement, mentionnons l’intention de publication des résultats de l’étude et le mécanisme de protection des données. J’ai insisté auprès des participants sur le fait qu’il n’y avait pas de participation forcée, mais seulement par des moyens volontaires. J’ai rappelé aux participants le droit d’arrêter et de retirer leur participation à tout moment. Aucune explication n’était requise pour se retirer, si ce n’est un simple courriel informant le chercheur de la décision de cesser de fumer.

Le consentement éclairé est un aspect crucial de toute étude de recherche donnée. Un chercheur devra équilibrer l’interaction des participants pour respecter toutes les exigences éthiques attendues d’une étude de recherche (Humphreys, 2015). Le chercheur

doit s'assurer que le processus de consentement éclairé ne viole pas les droits ou le respect des participants. Le consentement garantit le respect intégral de toutes les normes éthiques nécessaires (Greenwood, 2016). En tant que chercheur, j'ai suivi les exigences éthiques et légales de la CISR de l'Université Walden pour éviter de nuire aux participants à la recherche. La sécurité, la dignité et la voix des participants à l'étude sont essentielles pour garantir des pratiques éthiques lorsqu'ils entreprennent des recherches qualitatives (Wallace et Sheldon, 2015). Le consentement éclairé stipule que tous les participants à la recherche le font volontairement. Comme il est clairement indiqué dans le formulaire de consentement éclairé, les participants n'ont reçu aucune incitation sous forme de paiements pour qu'ils fassent participer à l'étude.

La confidentialité des participants à la recherche doit toujours être maintenue pour garantir l'intégrité de l'étude (Wallace et Sheldon, 2015). Yang et coll. (2018) ont noté que l'utilisation d'identificateurs uniques pour représenter les participants à l'étude protège le statut professionnel des participants. J'ai utilisé des lettres et des chiffres pour identifier les participants sur les relevés de notes et le registre de recherche. J'ai attribué des codes aux participants en fonction de leur ordre d'entrevue afin que le code « M 1 » représente la première personne interrogée, le code « M2 », le second, etc. J'étais la seule personne à avoir accès aux données de l'étude. J'ai stocké les données dans un lecteur externe protégé par mot de passe, qui a été conservé en toute sécurité pendant cinq ans pour se prémunir contre la confidentialité du participant.

Collecte de données

Instruments

En tant que chercheur, j'ai assumé le rôle de l'instrument principal de collecte de données et j'ai recueilli des données dans le milieu naturel. Selon Stacey (2016), les chercheurs qui entreprennent des études qualitatives assument le rôle d'instruments de collecte de données primaires. La collecte de données qualitatives nécessite d'établir la confiance avec les participants, ce qui signifie que le chercheur est l'instrument de collecte de données qui devrait élaborer une stratégie qui développera la crédibilité auprès des participants (Daniel, 2018). La collecte de données dans le milieu naturel aide les chercheurs à effectuer une analyse de données inductives et déductives en ce qui concerne l'établissement des thèmes et des modèles (Fletcher, 2017).

La collecte de données dans le cadre de la recherche qualitative peut se faire sous la forme d'entrevues semi-structurées et d'analyses de documents (Akaeze, 2016; Conrad et Tucker, 2019). Selon Van der Berg et Struwig (2017), les entrevues semi-structurées sont valides pour la collecte de données. Comme Farooq et de Villiers (2017) l'ont noté, les questions ouvertes offrent l'occasion à un chercheur entreprenant une étude de cas d'avoir une excellente idée des aspects spécifiques impliqués. Les questions d'entrevue que j'ai utilisées étaient ouvertes pour donner de la place à une interaction plus importante qui incluait les participants. J'ai analysé les documents des organisations pour effectuer une triangulation méthodologique. Outre les entretiens et les observations, j'ai utilisé les documents publiés et non publiés de l'organisation à but non lucratif tels que les statuts de l'organisation, le plan stratégique, la brochure, la politique, les journaux de

formation et le plan de sécurité du système. J'ai utilisé les entrevues comme instrument de collecte de données. J'ai utilisé un ensemble prédéterminé de questions d'entrevue comme instrument de collecte de données (annexe). Chaque personne interrogée a répondu au même ensemble de questions et dans le même ordre afin d'assurer l'uniformité des données recueillies.

Un chercheur peut obtenir différentes réponses et interactions au cours d'une séance d'entrevue s'il pose à différents participants les mêmes questions d'entrevue (Cataldi, 2018). Pandey et Chawla (2016) ont observé que les formats d'entrevue semi-structurés permettent aux participants d'avoir une compréhension approfondie du sujet de recherche. Ils ont également noté que l'adoption d'entrevues semi-structurées offre une approche accessible, souple et intelligible de la collecte de données. Muhammad (2018) a illustré le degré d'efficacité des études qualitatives à l'aide d'entretiens semi-structurés. Essentiellement, à l'aide d'entrevues semi-structurées, un chercheur peut divulguer des aspects cachés qui sont caractéristiques du comportement humain et organisationnel parce que les réponses des participants sont de telle manière qu'elles conviennent le mieux à la question d'entrevue.

J'ai posé les mêmes questions d'entrevue à tous les participants afin d'assurer la crédibilité et la fiabilité à l'aide d'un protocole d'entrevue (annexe). Selon Azungah (2018), poser les mêmes questions d'entrevue à tous les participants à la recherche aide à découvrir des thèmes. Lorsqu'il pose les mêmes questions de façon séquentielle, le chercheur peut entreprendre une analyse efficace des données et établir des comparaisons des réponses (Akaeze, 2016). Les chercheurs doivent éviter de poser des questions

principales parce que, selon Teixeira et coll. (2017), de telles questions favorisent les préjugés.

La triangulation méthodologique offre à un chercheur l'occasion d'atténuer les biais à mesure qu'il acquiert la capacité de voir les données sous divers angles. Ils peuvent considérer un phénomène de multiples façons (Fusch et coll., 2018). L'utilisation de la triangulation méthodologique améliorera davantage la souplesse dans l'établissement des tendances tout au long du processus d'analyse des données (Mason, 2018). L'utilisation de plusieurs sources de données comme cible de triangulation méthodologique améliore la crédibilité, la validité et la fiabilité de l'étude (Fusch et coll., 2018). J'ai combiné les entretiens des participants avec des documents d'organisation analysés tels que les documents publiés et non publiés des organisations à but non lucratif: règlements administratifs, plan stratégique, brochure, journaux de formation et plan de sécurité du système, journaux de formation, documents d'acquisition de logiciels et documents de politique. En accordant à Das et coll. (2018), les données archivées telles que les enregistrements et les documents mènent à des données de recherche qualitative précieuses. L'analyse par un chercheur de documents d'archives combinée à des observations et à des entrevues permet de faire la révélation de thèmes de recherche (Davidson et coll., 2019). La triangulation méthodologique, qui implique l'utilisation de plusieurs formes de données, permet à un chercheur de comprendre le fait qu'il étudie. Selon Fusch et coll. (2018), l'utilisation d'une combinaison de deux méthodes de collecte de données rend les données plus fiables, ce qui rend le cas plus compréhensible. La triangulation méthodologique facilite en outre l'exploration des tendances dans les

données, permettant au chercheur d'interpréter de multiples perspectives. L'adoption de la triangulation méthodologique renforce la confiance envers les résultats de l'étude, car elle implique l'utilisation de diverses sources qui, à leur tour, aident le chercheur à atténuer les biais de recherche (Azungah, 2018).

J'ai appliqué la vérification des membres dans le processus d'entrevue pour améliorer la validité de la recherche et réduire les préjugés. Grâce à la vérification des membres, Daniel (2018) a soutenu que le chercheur a une chance d'atteindre la rigueur ou la rigueur dans les études de cas. Les participants ont eu l'occasion d'examiner et de confirmer mon interprétation de la réunion initiale avant que je ne poursuive. Comme Daniel l'a fait remarquer, la vérification des membres offre une occasion pour le chercheur de vérifier le niveau d'exactitude de la réponse d'un participant. La vérification des membres sert également de processus de contrôle de la qualité, où le chercheur peut confirmer, clarifier et compléter les données obtenues à partir d'une entrevue de recherche qualitative (Iivari, 2018). J'ai utilisé un ensemble prédéterminé de questions d'entrevue comme instrument de collecte de données. Toutes les personnes interrogées ont répondu à la même série de questions et dans le même ordre afin d'assurer l'uniformité des données recueillies (Annexe).

Technique de collecte de données

Cette étude a utilisé les entrevues comme technique de collecte de données. L'entrevue comprend une méthode de collecte de données où les expériences des individus sont exploitées au moyen d'une séance de questions-réponses afin d'établir une compréhension composite qui élargit nos connaissances professionnelles (Quinney et

coll., 2016). Les chercheurs utilisent les entrevues pour saisir les expériences des participants dans les études qualitatives (Holland, 2017). Les chercheurs qui choisissent l'option d'une conversation comme technique pour interagir avec les participants peuvent utiliser des versions structurées, semi-structurées ou non structurées pour la collecte de données (McTate et Leffler, 2017). J'ai utilisé des entrevues semi-structurées et l'analyse de documents dans cette étude. J'ai cherché des documents d'organisation à analyser à partir des sites Web respectifs des organisations et j'ai demandé des données privées à des organisations à but non lucratif. Parmi les documents que j'ai recherchés sur les sites Web et que j'ai utilisés pour la collecte de données, mentionnons les journaux de formation, les documents d'acquisition de logiciels, les plans de sécurité du système et les documents de politique.

Les chercheurs qui utilisent des entrevues semi-structurées adoptent un guide pour l'entrevue où les questions énumérées se concentrent sur la capture du repère social de l'entrevue (Van Rooy et coll., 2015). Akaeze (2016) a expliqué que les chercheurs qui adoptent des entrevues semi-structurées dépendent de la question de recherche générale pour guider le processus de collecte de données. L'avantage des entrevues semi-structurées comprend la flexibilité d'utiliser des questions de suivi et de soutien, ce qui assure l'utilisation de données riches sur un phénomène. De plus, les entrevues semi-structurées comportent des questions ouvertes qui offrent aux participants la possibilité de répondre librement en utilisant leurs propres mots et en fonction de leur vision du monde (Kallio et coll., 2016). Les entrevues semi-structurées profitent également aux chercheurs grâce, selon Kallio et coll., à l'occasion de développer des relations avec les

participants. Une telle relation permet également au chercheur de répondre facilement aux préoccupations ou aux questions soulevées par les participants (Newton, 2017).

Les entrevues structurées comportent une configuration plus rigide en ce qui concerne la formulation et l'enchaînement des questions (Doll, 2017). Je n'ai pas choisi une entrevue structurée dans cette étude parce qu'elle impliquait des procédures rigoureuses, plus normalisées et avec des questions ordonnées. D'autre part, les entrevues non structurées exigent des chercheurs qu'ils posent différentes questions à différents participants en fonction du jugement du chercheur (Mcintosh et Morse, 2015). Je n'ai pas choisi les entrevues non structurées parce que, pratiquement, l'intervieweur a le pouvoir discrétionnaire de diriger le processus d'entrevue dans la direction qu'il préfère, ce qui, essentiellement, facilite les préjugés (Mcintosh et Morse, 2015).

Selon Holland (2017), cependant, les entrevues semi-structurées ont l'inconvénient d'être longues et coûteuses. La méthodologie non structurée, jumelée à la complexité des données et aux détails excessifs attribués aux participants, rend l'utilisation de la méthode assez difficile. De plus, l'utilisation d'entrevues semi-structurées augmente les risques de biais des chercheurs, ce qui peut, à son tour, influencer injustement l'interprétation des données(Brown et Danaher, 2017). J'ai invité les participants par courriel, en leur demandant de participer à l'étude. Les participants ont reçu, examiné et finalement approuvé un formulaire de consentement avant de participer. Le formulaire de consentement expliquait le processus de retrait, la divulgation des incitatifs et le mécanisme de protection des données.

J’ai utilisé le processus de vérification des membres pour m’assurer que j’obtenais la validité de la réponse. J’ai résumé toutes les réponses à l’entrevue pour la vérification des membres. Selon Madill et Sullivan (2018), la vérification des membres facilite la recherche des chercheurs dans leur quête d’étudier et d’adapter leur interprétation relativement aux réponses des participants. J’ai engagé une conversation de vérification des membres avec les participants pour leur permettre d’examiner et de confirmer mon interprétation de leurs réponses. On a demandé aux participants de modifier, de simplifier, d’expliquer davantage et de commenter le résumé de leur réponse pour s’assurer que je comprends leur point de vue.

Techniques d’organisation des données

Les chercheurs utilisent souvent des logiciels pour suivre les données et les organiser en conséquence (Che-Hung et coll., 2017). Après les entretiens, j’ai transféré les données brutes dans NVivo. J’ai également supprimé tous les éventuels détails personnels ou identifiables qui pourraient rapidement révéler l’identité réelle des participants. J’avais un dossier avec des étiquettes relatives à chaque étude de cas, où je stockais les transcriptions, les notes et les enregistrements d’entrevue dans un lecteur externe qui ne m’était accessible que pendant cinq ans. Je l’ai fait pour améliorer la vie privée et la sécurité des participants.

En entreprenant l’analyse des données, j’avais l’intention d’effectuer une évaluation plus approfondie des thèmes et des tendances des entrevues. J’ai téléchargé, organisé et analysé les données d’entrevue transcrites à l’aide du logiciel NVivo. En tant que logiciel assisté par ordinateur pour l’analyse qualitative des données, le logiciel

NVivo facilite la collecte de données et la gestion et l'analyse subséquentes. À l'aide du logiciel NVivo, j'ai reconnu des unités significatives, élargi des thèmes émergents, géré des données et entrepris une triangulation.

J'ai chargé les documents publiés et non publiés des organisations à but non lucratif tels que le plan de stratégie de l'organisation, la brochure et la politique dans le logiciel NVivo à des fins de triangulation méthodologique. La triangulation méthodologique m'a donné l'occasion d'utiliser de multiples sources de données de recherche qualitative. Mon utilisation de la triangulation méthodologique m'a aidé à atteindre la flexibilité en termes de détermination des tendances au cours de l'analyse des données. De multiples sources de données fournissent une triangulation méthodologique à l'appui d'un argument plausible de la solidité des résultats de recherche, des conclusions et des recommandations (Heesen et coll., 2016).

J'ai utilisé le codage des données pour simplifier le processus de comparaison et de reconnaissance des modèles. En codant les données qualitatives, j'ai étudié les données d'étude pour les catégories, les idées et les thèmes communs. Le codage a facilité l'analyse, l'organisation et la comparaison des données pour permettre l'extraction d'informations significatives. J'ai appliqué un processus de codage qui classait les données en fonction des types de sources à l'aide de documents archivés et d'entrevues pour déterminer les thèmes émergents (Young et coll., 2018).

Lorsque vous utilisez NVivo pour coder des données, des nœuds doivent être créés (Ballaro &Polk, 2017). Un nœud constitue les références collectées sur un thème, une personne, un domaine d'intérêt ou un lieu spécifique. J'ai utilisé des transcriptions,

des journaux et des notes pour découvrir des thèmes inhérents, des modèles et déduire des significations en fonction des réponses des participants. J'ai pris des notes d'entrevue sous la forme d'un journal de recherche pour assurer la conformabilité, la validité et la fiabilité de mon étude. Mohajan (2018) est d'avis que les chercheurs s'appuient délibérément sur les journaux de recherche pour saisir des données et examiner les hypothèses et les actions qui sont thématiques dans une étude donnée. Les journaux de recherche offrent en outre une piste d'audit précieuse pour assurer la conformabilité et permettre au chercheur de reconnaître et de réfléchir aux défis potentiels susceptibles d'affecter la recherche (Mohajan, 2018).

Technique d'analyse des données

Selon Assarroudi et coll. (2018), l'analyse des données constitue un processus de classification de l'information recueillie lors des séances d'entrevue, ou par observation, ou l'examen de documents visuels et écrits. Je me suis lancé dans la transformation des données brutes et leur organisation en conséquence pour atteindre la rigueur dans l'analyse des données. J'ai veillé au respect de l'analyse des données en respectant tous les principes standard, y compris la transcription des entrevues, l'analyse complète du phénomène à l'étude, la vérification par les membres du développement du codage des données et la détermination des liens avec les thèmes. Nowell et coll. (2017) ont expliqué que le processus d'analyse des données survient après que le chercheur accède au domaine, recueille des données et les transcrit.

J'ai téléchargé, organisé et analysé les données d'entrevue transcrites à l'aide du logiciel NVivo. En tant que logiciel assisté par ordinateur pour l'analyse qualitative des

données, NVivo facilite la collecte de données et la gestion et l'analyse subséquentes de données qualitatives telles que le contenu écrit et audio (Woods et coll., 2016). À l'aide du logiciel NVivo, j'ai reconnu des unités significatives, élargi des thèmes émergents, géré des données et entrepris une triangulation. En utilisant à la fois les données d'entrevue et d'analyse de documents, j'ai réalisé une triangulation méthodologique et une flexibilité dans la détermination des tendances de l'analyse des données. De multiples sources de données fournissent une triangulation méthodologique à l'appui d'un argument plausible en faveur de la solidité des résultats de recherche, des conclusions et des recommandations (Nowell et coll., 2017).

J'ai utilisé le codage des données pour simplifier le processus de comparaison et de reconnaissance des modèles. En codant les données qualitatives, j'ai étudié les données d'étude pour les catégories, les idées et les thèmes communs (Wu et al., 2016). Le codage a facilité l'analyse, l'organisation et la comparaison des données pour permettre l'extraction d'informations significatives. J'ai appliqué un processus de codage qui classait les données en fonction des types de sources à l'aide de documents archivés et d'entrevues pour déterminer les thèmes émergents (Erlingsson et Brysiewicz, 2017).

Fiabilité et validité

Introduction

En général, la recherche qualitative doit établir la fiabilité des données pour en assurer la fiabilité et la validité (Roberts et coll., 2019). Il est essentiel pour un chercheur de porter une attention particulière lors de la conception d'une étude pour s'assurer que les résultats sont bien applicables. L'utilisation de la transférabilité, de la fiabilité et de la

confirmabilité facilite l'établissement de la fiabilité et l'amélioration de la qualité d'une étude (DeGama et coll., 2019). Les études qualitatives pour atteindre la fiabilité si nécessaire doivent être crédibles, fiables, confirmables et transférables (DeGama et coll., 2019).

Fiabilité

Dans la recherche qualitative, la fiabilité fait référence à la façon dont les données sont reproductibles et stables (Leung, 2015). La vérification des membres est un élément essentiel pour déterminer si le chercheur étudie et interprète avec précision les réponses des participants (Madill et Sullivan, 2018). J'ai donné l'occasion aux participants de vérifier mon interprétation de leurs réponses à l'entrevue afin d'assurer l'exactitude des conclusions. De plus, la vérification des membres diffuse les analyses et les réponses de recherche des participants afin d'en saisir le sens et d'accroître la fiabilité des données (Fusch et coll., 2018). Selon Robins et Eisen (2017), la triangulation se traduit également par une fiabilité dans la recherche. La triangulation utilise de nombreux appuis de données afin de maintenir les données d'entrevue et d'assurer la fidélité des résultats de la recherche. J'ai utilisé plusieurs sources de collecte de données telles que des documents publiés et non publiés et des entretiens semi-structurés pour assurer la fiabilité des résultats.

Validité

Fiabilité

La fiabilité implique la mesure dans laquelle les résultats de la recherche sont produits de manière éthique et précise (Van der Ber. &Struwig, 2017). Les chercheurs

atteignent la fiabilité des données en vérifiant les membres, car cela aide à s'assurer que leurs préjugés personnels n'influencent pas les données recueillies (Akaeze, 2016). Dans cette étude, j'ai authentifié les conclusions à l'aide de la vérification des membres ainsi que des méthodologies de triangulation. En ce qui concerne la vérification des membres, j'ai principalement diffusé les interprétations et les réponses de recherche des participants immédiatement après le processus de collecte des données, en les invitant à les valider. En ce qui concerne la triangulation, j'ai recoupé toutes les données résultant de l'entrevue et de l'analyse des documents. Je me suis accroché aux données attribuées aux participants à la recherche et je n'ai pas tenu compte des opinions personnelles susceptibles d'entraîner des biais.

L'importance de la fiabilité réside dans le fait qu'elle améliore la fiabilité des résultats (Nowell et coll., 2017). J'ai atteint la fiabilité dans mon étude avec l'enregistrement audio et la rédaction des réponses pendant l'entrevue. J'ai ensuite transcrit les informations et utilisé le logiciel Nvivo pour analyser les données résultantes.

Crédibilité

La crédibilité implique le degré ou l'étendue de l'objectivité et de l'impartialité des résultats de la recherche (Bradshaw et coll., 2017). La crédibilité garantit que les chercheurs font correspondre efficacement les opinions des participants avec les résultats finaux (Colorafi et Evans, 2016). Selon Turner et Baker (2019), les chercheurs recherchent la crédibilité dans leurs études comme moyen d'atteindre la fiabilité et l'intégrité nécessaires. La crédibilité est un aspect essentiel des données qualitatives internes et implique l'établissement de résultats de recherche plausibles selon le point de

vue des participants à la recherche (Noble et Smith, 2015). Une étude jugée crédible implique que les examinateurs qui ne participent pas à l'étude reconnaissent ses résultats et que les résultats demeurent applicables à d'autres milieux ou groupes (Noble et Smith, 2015).

Iivari (2018) a décrit la vérification des membres comme une procédure de contrôle de la qualité entreprise dans le cadre de la recherche qualitative pour permettre au chercheur de confirmer, d'expliquer ou d'accroître l'exactitude de l'exactitude relative aux données d'entrevue recueillies. La vérification des membres assure une vérification adéquate des données obtenues lors des entretiens. Daniel (2018) a noté que la vérification des membres permet aux participants de valider la représentation des réponses.

Transférabilité

La transférabilité fait référence à la capacité de généraliser les résultats de la recherche à une population plus large. Pour atteindre la transférabilité, il faut qu'un chercheur qualitatif trouve un sens à une personne impliquée dans la recherche (Gammelgaard, 2017). L'utilisation de l'échantillonnage téléologique, comme le soulignent Venkatesh et coll. (2016), pourrait améliorer la transférabilité. De plus, la triangulation méthodologique aide à améliorer la transférabilité (Fusch et coll., 2018). Ma structure de recherche comprenait un échantillonnage ciblé et un aperçu complet des hypothèses, des délimitations et des limites de la recherche. La structure a fourni un contexte adéquat pour établir la transférabilité de cette étude par d'autres chercheurs. J'ai enregistré les résultats de la recherche afin que d'autres chercheurs puissent les

reproduire en utilisant des descriptions épaisses pour illustrer les données des participants et en incluant des exemples bruts de données. J'ai utilisé la triangulation méthodologique en plus de maintenir une base de données d'études de cas qui comprenait des données brutes, à thème, triées et interprétatives.

Confirmabilité

La confirmabilité de la recherche fait référence à la façon dont d'autres peuvent corroborer les résultats de la recherche (Muhammad, 2018). Les chercheurs peuvent utiliser des revues réflexives, l'enregistrement et l'examen des relevés de notes, la vérification des membres, ainsi que la prise de notes dans le processus d'entrevue pour saisir la piste d'audit afin d'assurer la confirmabilité et la fiabilité de la recherche qualitative (DeGama et coll., 2019). La confirmabilité permet de s'assurer que le chercheur signifie les réponses des participants par opposition au biais du chercheur. J'ai atteint la confirmabilité et la fiabilité en enregistrant les transcriptions, en les examinant et en effectuant la vérification des membres et en prenant des notes tout au long du processus d'entrevue.

Transition et résumé

Dans la section 2, j'ai couvert de nombreux éléments essentiels qui constituent cette étude, y compris la reformulation de l'énoncé de l'objectif et l'élaboration du rôle du chercheur. J'ai également discuté des participants à l'étude, analysé la méthode de recherche et sa conception, l'échantillonnage de la population, l'éthique dans la recherche, les instruments de collecte de données, les techniques de collecte de données, l'analyse des données, la question de la fiabilité et de la validité, et enfin, le résumé de la

transition. Dans la section 3, j'ai donné un aperçu de l'étude, présenté les résultats, appliqué les résultats à la pratique professionnelle, couvert les répercussions sur le changement social, fourni des recommandations d'action, fourni des recommandations pour une étude plus approfondie, offert des réflexions et, enfin, résumé et inclus l'étude de conclusion.

Section 3 : Application à la pratique professionnelle et répercussions sur le changement

Aperçu de l'étude

Dans cette étude de cas qualitative multiple, j'ai cherché à étudier les stratégies que les ISSM emploient dans les organisations à but non lucratif pour se protéger contre les cyberattaques. La population de recherche comprenait cinq responsables informatiques et directeurs travaillant dans des organisations à but non lucratif présentant les caractéristiques suivantes: (a) autorisé à opérer légalement dans l'État du Maryland, le district de Columbia et la Virginie; b) employait au moins 150 personnes; c) a mis en œuvre efficacement des mesures de cybersécurité et d) a enregistré des recettes brutes annuelles d'au moins 5 millions de dollars. L'étude était fondée sur la TPS comme cadre conceptuel. Au cours de la séance d'entrevue et de l'examen de la documentation archivistique de l'entreprise, les réponses des participants ont contribué à toutes les données pour répondre à la question de recherche. Les principaux thèmes qui ont résulté des données recueillies étaient a) la stratégie de cybersécurité, b) la sensibilisation à la cybersécurité et c) la dépendance à l'égard des fournisseurs de services d'infrastructure tiers. Dans mon analyse des résultats de l'étude, j'ai cherché à déterminer les principales stratégies que les ISSM dans les organisations à but non lucratif emploient pour se protéger contre les cyberattaques.

Présentation des constatations

J'ai voulu que la question de recherche principale de cette étude détermine les stratégies que les ISSM des organisations à but non lucratif utilisent pour se protéger contre les cyberattaques. J'ai utilisé des questions d'entrevue semi-structurées ouvertes

(annexe) et des documents d'archives pour recueillir des données pour l'étude. J'ai déterminé l'atteinte de la saturation des données lorsque les données des répondants à l'entrevue et les documents d'archives de l'entreprise sont devenus répétitifs. En tant que chercheur et principal instrument de collecte de données, j'ai créé une base de données et tenu une piste de vérification de la correspondance et de la documentation archivistique des participants. J'ai utilisé QSR International NVivo pour analyser les données de recherche. J'ai importé toutes les réponses recueillies au cours des séances d'entrevue, les notes d'entrevue, la documentation archivistique de l'entreprise et les fichiers d'interprétation vérifiés par les membres.

L'analyse des documents d'archives des organismes sans but lucratif, y compris les politiques organisationnelles et les rapports d'affaires, a corroboré les réponses des participants aux entrevues. J'ai utilisé des pseudonymes pour chaque participant comme P1, P2, P3, P4 et P5. Le participant 1 provenait de l'organisation 1, tandis que le participant P2 provenait de l'organisation 2, le participant 3 de l'organisation 3, le participant 4 de l'organisation 4 et le participant 5 de l'organisation 5. Les trois thèmes qui se sont dégagés de l'analyse étaient les suivants : a) sensibilisation à la cybersécurité, b) stratégie de cybersécurité et c) dépendance à l'égard du tiers. Le tableau 1 illustre les trois grands thèmes et les références respectives.

Tableau 1

Thèmes et leurs références respectives

Thèmes principaux	Participants	Réponse (%)	Documents	Références
Sensibilisation à la cybersécurité	5	100	30	68
Stratégie de cybersécurité	5	100	25	44
Dépendant du tiers	5	100	8	52

Note. Les références illustrent la fréquence à laquelle les participants ont mentionné les thèmes.

Thème 1 : Sensibilisation à la cybersécurité

Les sous-thèmes pertinents sous la sensibilisation à la cybersécurité sont la violation de données, la compréhension de la protection, la compréhension des plans stratégiques et la compréhension des fournisseurs tiers. Le tableau 2 met en évidence les sous-thèmes du thème de sensibilisation à la cybersécurité.

Tableau 2

Sous-thèmes du thème sensibilisation à la cybersécurité

	Participants		Documents	
Thèmes majeurs/mineurs	Compter	Références	Compter	Références
Violation de données	5	17	3	7
Présentation de la protection	5	17	9	14
Comprendre les plans stratégiques	5	12	10	27
Présentation des fournisseurs tiers	5	13	8	16

Violation de données

L'atteinte à la protection des données fait référence à l'accès non autorisé à des données confidentielles, telles que les données des clients, à des fins d'exploitation (Kude et coll., 2017). Les auteurs de violations de données peuvent être des acteurs internes de l'organisation, tels que des employés, ou des acteurs externes tels que des pirates informatiques. En fonction des réponses des participants, les organisations doivent établir des stratégies pratiques de protection contre les atteintes à la protection des données. Trois documents d'archives utilisés dans l'étude ont souligné l'importance d'utiliser des stratégies uniques pour traiter les atteintes à la protection des données au sein de l'organisation. P1 a indiqué qu'elle s'attaque aux atteintes à la protection des données dans l'organisation en scannant les courriels et en évitant de répondre à ces courriels. Un document de politique de l'organisation 1 a souligné que « l'organisation dispose d'une équipe d'atteinte à la protection des données établie dirigée par le directeur informatique, avec le mandat de prendre des décisions critiques de tous les temps concernant la gestion et le confinement des incidents de violation de données ». Sur la base de la réponse de P1 et des preuves présentées dans le document de politique de l'organisation, il est évident que l'organisation comprend à quel point les violations de données peuvent être dangereuses dans la perte et l'exploitation d'informations, d'où la nécessité d'analyser les e-mails et d'avoir une équipe de violation de données prête à s'assurer qu'ils sont en sécurité.

P3 a déclaré : « Nous avons une équipe de sécurité qui est dirigée par l'un de nos partenaires, et elle est responsable d'au moins garder une trace de notre posture de sécurité. Nous n'avons pas comme un endroit centralisé où nous aimons surveiller tout

notre trafic d'infrastructure. D'après la réponse de P3, la stratégie claire de l'organisation repose sur une équipe de sécurité chargée d'évaluer continuellement sa position en matière de sécurité pour contrôler ou éviter les violations de données. Pour P4, leur approche consistait à embaucher une entreprise externe qui effectue des audits et des évaluations des risques en leur nom. Sur la base des résultats de l'audit et de l'évaluation, l'entreprise détermine son rendement en ce qui concerne les atteintes à la protection des données en cause. Un document de politique de l'organisation 4 indiquait que l'organisation collaborerait avec des entreprises de TI expertes externes pour cerner les lacunes potentielles en matière d'atteinte à la protection des données dans les systèmes de l'organisation et agir de façon décisive pour mettre fin à l'atteinte.

> P5 suite,
>
> Nous examinons le journal de vérification, nous examinons l'événement de sécurité, nous examinons le registre de sécurité, nous examinons les adresses IP étranges provenant d'appareils sans fil, nous examinons l'heure de la journée et nous examinons toutes les activités suspectes qui se déroulent à une certaine période.

Un document de politique de confidentialité et de sécurité de l'organisation 5 indiquait : « Un logiciel de prévention des fuites de données (DLP) devrait être utilisé en tout temps pour aider l'organisation à contrôler les atteintes à la protection des données en tout temps. » La réponse de P5, ainsi que les preuves du document d'archives, révèlent que l'organisation utilise divers indicateurs vitaux pour contrôler les violations de données en tout temps.

Les réponses des participants ont souligné les observationsde Daniel Ani et coll. (2016) selon lesquelles la gestion et le contrôle des atteintes à la protection des données sont un aspect essentiel de la sensibilisation à la cybersécurité dans toute organisation. Les réponses des participants ont renforcé le point de vue de Gordon et coll. (2015) selon lequel les organismes à but non lucratif, tout comme les organismes à but lucratif, doivent régir leurs données pour garantir une sensibilisation suffisante à la cybersécurité. Une fois qu'une organisation à but non lucratif améliore ses capacités internes pour protéger et garantir des données de haute qualité tout au long du cycle de vie des données, elle atteint la sécurité, l'intégrité, la cohérence et la disponibilité des données (Daniel Ani et al., 2016).

Les données tirées des réponses des participants et de la documentation à l'appui étaient conformes au concept de la TPS en ce qui a trait à la proposition de meilleurs systèmes organisationnels qui améliorent l'efficience. D'après la description de la TPS par Chen et coll. (2012), les systèmes peuvent interagir en collaboration et se rapporter pour former un système supérieur qui s'avérera difficile à manipuler facilement par des pirates informatiques. Selon Gordon et coll. (2015), les atteintes à la cybersécurité résultent principalement d'un manque de sensibilisation au système d'information, ce qui amène les employés à se faire des erreurs dans le partage de leurs informations de connexion, l'envoi d'informations classifiées aux destinataires involontaires, etc. Les réponses de P1, par exemple, ont montré des preuves d'un système établi dans l'organisation utilisé de manière holistique pour suivre et supprimer les e-mails nuisibles qui peuvent causer une violation de données.

Présentation de la protection

Comprendre la protection en termes de sensibilisation à la cybersécurité signifie reconnaître l'importance de la protection des données au sein de l'organisation. Au cours des entrevues, trois des participants ont mentionné les efforts déployés dans leurs organisations respectives pour protéger les données stockées. P1 a déclaré: « Nous essayons de travailler sur et de protéger nos données et de protéger notre organisation. » Un document organisationnel de l'organisation 1 mentionnait que « tous les dépôts de données au sein de l'organisation ont un accès contrôlé qui permet uniquement à ceux qui ont les bonnes informations d'identification d'y accéder ». Cette réponse, ainsi que les preuves documentaires, ont reconnu les efforts déployés par l'organisation pour protéger les données de l'organisation, car les données sont une ressource essentielle nécessitant une protection totale à tout moment pour éloigner les pirates informatiques. Comprendre la protection est un aspect essentiel de la sensibilisation à la cybersécurité. Un ISSM dans une organisation à but non lucratif doit évaluer et déterminer si le risque associé à l'externalisation des opérations de protection de la sécurité de l'organisation à une entité tierce l'emporte sur les pertes organisationnelles. De même, P4 a déclaré : « Notre direction a coopéré avec nous pour nous donner suffisamment de ressources pour protéger l'organisation. » Un document officiel de l'organisation 4 se lit en partie comme suit : « Le gestionnaire de données doit s'assurer que le système de l'organisation, y compris les ordinateurs, les bases de données et les options de stockage de données amovibles, a la pleine capacité d'assurer l'intégrité des données. » Sur la base de la réponse de P4 et des détails du document officiel de l'Organisation 4, l'organisation avait

hiérarchisé les plans pour assurer la protection des données. La direction est l'organe décisionnel principal dans la plupart des organisations, et leur implication dans la protection des données est cruciale pour garantir la sensibilisation à la cybersécurité.

P5 a affirmé : « L'autre façon dont nous protégeons nos informations à notre disposition est que nous encourageons les employés à ne pas créer un document sensible et à le laisser sur l'imprimante réseau où n'importe qui peut simplement entrer et le récupérer. » Un document de politique de confidentialité et de sécurité de l'organisation 5 indiquait : « Tous les employés doivent avoir un mot de passe unique qui leur permet de s'aventurer dans le système et d'interagir avec les données. » En analysant les réponses et les preuves documentaires, il était clair que les employés jouent un rôle important dans la cybersécurité dans l'organisation. Toutes les règles et politiques de sécurité de l'organisation n'ont plus de sens si les employés n'assument pas la responsabilité de les apprendre et de les mettre en œuvre efficacement. Les ISSM dans les organisations doivent se concentrer sur les employés pour s'assurer qu'ils créent une sensibilisation suffisante à la cybersécurité. La cyberattaque constitue un défi important pour les organisations qui tentent de protéger leurs données contre la disparition. Plusieurs systèmes tels que le système de prévention des intrusions, le système de détection des intrusions, les périphériques de mise en forme de paquets, les pare-feu, etc., sont utilisés pour protéger les réseaux.

Les réponses des participants soulignent l'importance pour les employés et les organisations à but non lucratif dans leur ensemble de comprendre l'essence de la protection dans la réalisation de la cybersécurité. Selon Mierzwa et Scott (2017), la

plupart des organisations à but non lucratif font les frais des violations de données et des interférences de pirates informatiques en raison du financement limité accordé au développement et au contrôle informatiques. Le manque de financement s'est traduit par une mauvaise connaissance ou compréhension de la protection dans la plupart des organisations. Jagalur et coll. (2018) ont conclu que les organismes sans but lucratif ont une compréhension limitée de la cybersécurité en raison de leur manque de spécialités en cybersécurité pour prendre en charge leurs unités informatiques. Lorsqu'une organisation n'a pas une bonne compréhension de la cybersécurité, elle ne parvient pas à aligner ses objectifs sur les bonnes pratiques de cybersécurité. Les organismes sans but lucratif doivent mettre plus de sérieux dans la poursuite de la compréhension de la protection au sein de l'organisation afin d'améliorer leurs mécanismes de protection contre les violations de données et les pirates (Jagalur et al., 2018). Étant donné que de nombreuses organisations à but non lucratif traitent des données personnelles, elles doivent donner la priorité à la formation de leur personnel sur les mesures techniques et organisationnelles nécessaires en matière de sécurité pour accroître leurs connaissances en matière de protection (Dove, 2018). Ces connaissances en matière de protection de la cybersécurité permettront aux employés de comprendre et de mettre en œuvre efficacement des lois complètes sur la sécurité des données au profit de l'organisation.

Le concept de la TPS saisit généralement l'utilité de protéger un système parce qu'il souligne la nécessité d'une combinaison de stratégies pour assurer la sécurité des données. Selon le principe de Bertalanffy (1968), les cyberattaques constituent des phénomènes observables causant des problèmes sociaux aux organismes sans but lucratif.

La protection des organisations contre les effets des cyberattaques permet d'obtenir une base métascientifique qui fait partie de la systéologie générale. Dans la pratique, de nombreuses organisations établissent une politique commune sur la sûreté et la sécurité des données au lieu d'aller avec la motivation de chaque employé à mettre en œuvre des politiques de sécurité de l'information (Doherty&Tajuddin, 2018). Grâce à la formation des employés sur la sécurité des données, les organisations mettent en œuvre de façon proactive le principe de la TPS qui protège leurs systèmes contre l'exploitation des données (Doherty et Tajuddin, 2018). En tant que systèmes, les organisations doivent établir l'infrastructure nécessaire et adopter une culture matérielle imposant un comportement de protection parmi leurs employés (Kim et Kim, 2017). Parce que la cybersécurité est une situation dynamique, les organisations à but non lucratif doivent continuellement penser à établir des systèmes de protection pour encourager les employés à faire des efforts volontaires.

De plus, les organisations peuvent également s'appuyer sur différentes techniques de modélisation d'attaque pour soutenir leur compréhension de l'attaque. Les organisations doivent donner la priorité à la protection de leur réseau contre les attaquants. Les résultats de cette recherche appuient davantage le concept de la TPS, en particulier son aspect de la technologie des systèmes. La création de connaissances et de sensibilisation à la protection des données aide les organisations à protéger leurs précieuses données, car elle crée une harmonie entre les politiques, les logiciels, le matériel et la formation (Carrapico et Farrand, 2017).

Comprendre les plans stratégiques

La compréhension des plans stratégiques pour la sensibilisation à la cybersécurité augmente l'interprétation par les intervenants de l'organisation concernant les mesures tactiques à mettre en œuvre pour répondre à la sensibilisation à la cybersécurité. Le participant P2 a indiqué comment la compréhension des plans stratégiques aide à établir une sensibilisation à la cybersécurité. En particulier, le participant P2 a déclaré : « Le succès de tout programme de cybersécurité est ce que nous appelons un plan stratégique de cybersécurité. Certaines personnes pourraient l'appeler un plan de marge de cybersécurité ou un plan de gestion de la sécurité du système, mais le mot clé est la stratégie. De même, le document de politique de l'Organisation 2 se lisait en partie comme suit : « Les efforts de protection des données doivent commencer par la création d'informations, l'objectif principal étant la définition et la documentation des décisions de contrôle d'accès et des niveaux de protection. La protection doit être appliquée tout au long du cycle de vie des données. D'après la réponse complète de P2, aucun plan de cybersécurité n'est utile à l'organisation à moins qu'un plan stratégique ne soit établi. Le plan stratégique permet une meilleure compréhension de l'environnement et du profil, permettant à l'employé de connaître ses insuffisances et ses vulnérabilités. Sans plan stratégique, l'ISSM ne peut apporter les modifications nécessaires pour atteindre les résultats souhaités.

La réponse ci-dessus souligne l'aide que la planification stratégique de la cybersécurité permet d'atteindre pour atteindre les objectifs et les capacités tactiques des organisations. Efthymiopoulos (2019) a fermement épousé l'importance de la planification de la cybersécurité dans la réalisation d'objectifs et de capacités tactiques,

car elle atteint un cadre politique, une méthodologie, une orientation et une mise en œuvre pour toutes les questions relatives à Internet lorsqu'elle est interconnectée. La réponse illustre également comment les plans stratégiques jouent un rôle important dans l'amélioration de la sensibilisation à la cybersécurité au sein des organisations. Selon Efthymiopoulos (2019), la connaissance des plans stratégiques aide à projeter la criticité de la cybersécurité en termes de politique. Lorsque les employés d'un organisme à but non lucratif comprennent les plans stratégiques de cybersécurité, ils apprécient également l'importance de méthodes améliorées pour les opérations cyber dimensionnelles de l'organisation. L'organisation bénéficiera de nombreux éléments et variables de cybersécurité, ce qui se traduira par une stratégie de cybersécurité plus grande. Junior et Santos (2016) croyaient également que le plan stratégique de sécurité de l'information d'une organisation la positionne pour réduire, déplacer, accepter ou éluder les risques liés à l'information associés aux personnes, aux technologies et aux processus. Le plan de cybersécurité produit des propositions soulignant la nécessité d'établir une approche de cybersécurité intégrée.

Le plan stratégique de cybersécurité s'harmonise également avec la TPS. Selon le concept de TPS de Von Bertalanffy (1972), l'environnement externe échappe au contrôle d'une organisation en raison de nombreuses forces irrégulières telles que la technologie ou l'innovation, la concurrence et l'économie d'autres. Ces facteurs ou forces constituent des sous-systèmes qui constituent un système plus étendu. L'explication du modèle de planification stratégique par la TPS comprend donc la façon dont chacun des sous-systèmes interagit. En utilisant l'approche conceptuelle de la TPS, les ISSM en

apprennent davantage sur les tendances technologiques et d'innovation et sur la nature décisive de l'interaction entre ces diverses composantes.

Présentation des fournisseurs tiers

Les fournisseurs tiers sont des acteurs externes qui offrent des services informatiques que l'organisation peut ne pas fournir entièrement à partir de son service informatique interne. Comprendre les fournisseurs tiers est essentiel dans la quête de sensibilisation à la cybersécurité, car cela permet à l'organisation de déterminer sa capacité à s'aligner sur ses anticipations. Trois des participants ont illustré leur compréhension des fournisseurs tiers et leur importance pour la sensibilisation à la cybersécurité au sein de l'organisation. Par exemple, le participant P1 est d'avis que les fournisseurs tiers ont une connaissance plus approfondie de la cybersécurité, ce qui les aide à conseiller les organisations clientes chaque fois que des problèmes de sécurité surviennent. Cette réponse prouve dans quelle mesure les responsables de l'organisation font confiance à des fournisseurs tiers en fonction des connaissances qu'ils possèdent. Le document de politique de sécurité et de confidentialité analysé de l'organisation 1 a montré que l'organisation intégrerait l'expertise des fournisseurs tiers pour fournir ce que l'organisation ne peut pas fournir. Le participant P4, quant à lui, a affirmé que sa capacité à gérer sa cybersécurité interne était limitée en tant qu'organisation. Par conséquent, l'organisation comprend la nécessité d'externaliser des fournisseurs tiers avec des capacités et une expérience plus élevées pour garantir la sensibilisation à la cybersécurité parmi les employés.

De même, le participant P5 a expliqué que l'organisation travaille avec un système tiers élaboré en qui elle a confiance pour résoudre certains de ses problèmes internes liés à la cybersécurité. La confiance du système de fournisseur tiers est basée sur l'expertise des fournisseurs dans la gestion de la cybersécurité. Un document officiel de l'organisation 5 analysé dans le cadre de cette recherche expliquait que l'organisation se procurerait des services de fournisseurs tiers s'ils s'avéraient rentables et techniquement supérieurs à ce que l'organisation fournit à l'interne.

Ces réponses des participants à la recherche font écho à la position de Jagalur et coll. (2018) selon laquelle de nombreuses organisations à but non lucratif reconnaissent qu'elles n'ont pas la capacité optimale de sécuriser leur infrastructure et leurs services informatiques. Les réponses confirment également l'observation de Bauer et coll. (2017) selon laquelle la plupart des organisations à but non lucratif ont intégré des procédures et des politiques de sécurité qui intègrent les opérations de tiers. En règle générale, comme Bauer et al. (2017) l'ont ajouté, les fournisseurs tiers de confiance, la responsabilité limitée, la réduction des risques et la formation des fournisseurs constituent des mesures d'intervention critiques que les ISSM des organismes à but non lucratif utilisent lors de l'intégration de la gestion de la sécurité des fournisseurs tiers. Cependant, une organisation à but non lucratif doit comprendre les rôles et les capacités d'un fournisseur tiers avant de choisir d'intégrer son assistance pour améliorer la sensibilisation à la cybersécurité.

L'aspect philosophie du système de la TPS s'aligne sur la discussion sur les organisations à but non lucratif qui intègrent des fournisseurs tiers dans leur quête de

sensibilisation à la cybersécurité. De nombreuses organisations à but non lucratif investissent très peu dans leurs systèmes informatiques de base, laissant leurs systèmes largement exposés aux pirates qui utilisent des compétences et des technologies supérieures. Sur la base du concept de TPS, les organismes sans but lucratif comptent sur l'apport de fournisseurs tiers pour renforcer leurs systèmes et améliorer l'efficacité. Selon la théorie fondamentale de la TPS, les organisations peuvent établir des systèmes supérieurs protégés contre les pirates informatiques en utilisant de nombreux sous-systèmes provenant de fournisseurs tiers compétents.

Thème 2 : Stratégie de cybersécurité

Le thème de la stratégie de cybersécurité comprend quelques sous-thèmes de base : acquisition, audit, sensibilisation, plan de sécurité, procédures de sécurité et formation. La stratégie de cybersécurité fait référence au plan d'action global visant à améliorer la résilience de l'infrastructure organisationnelle en ce qui concerne la sécurité des TI (Pardini et coll., 2017). Une stratégie de cybersécurité hautement fonctionnelle doit constituer une approche de haut niveau qui définit un éventail d'objectifs organisationnels et de priorités à atteindre au cours d'une période déterminée (Bauer et coll., 2017). Le tableau 3 met en évidence les sous-thèmes du thème de la stratégie de cybersécurité.

Tableau 3

Sous-thèmes sous le thème de la Stratégie de cybersécurité

	Participants		Documents	
Thèmes majeurs/mineurs	Compter	Références	Compter	Références
Acquisition	5	19	1	6
Audit	5	24	3	13
Conscience	5	12	3	19
Plan de sécurité	5	7	7	10
Procédures de sécurité	5	65	5	12
Formation	5	28	6	42

Acquisition

L'acquisition fait référence à l'acquisition des outils et stratégies informatiques requis pour assurer la cybersécurité. Sur la base des réponses des participants, la budgétisation est essentielle à l'acquisition de stratégies de cybersécurité dans les organisations à but non lucratif. Un document d'archives de l'étude traitait directement de la budgétisation, ce qui était important pour les constatations. P1 a déclaré: « Nous arrivons avec un budget basé sur la croissance des données des années précédentes, et sur cette base, nous essayons de trouver plusieurs ce dont nous pensons avoir besoin. » Le document d'archives de l'organisation 1 indiquait en partie: « Le directeur informatique est responsable du processus de budgétisation de la cybersécurité, garantissant que l'entreprise en a pour son argent dans tous les outils de cybersécurité acquis. » Les preuves mises en évidence par P1 et corroborées par le document d'archives illustrent comment l'organisation priorise le processus budgétaire avant d'acquérir la stratégie de cybersécurité souhaitée.

P2 a mentionné qu'en tant qu'organisation, ils évaluent souvent leurs capacités en ce qui concerne les outils qu'ils possèdent. L'organisation peut planifier ses ressources en vue d'acquérir les outils appropriés en fonction des défis rencontrés précédemment dans le cas d'une telle évaluation. D'après la réponse de P2, il est clair que l'organisation aligne son acquisition de cybersécurité avec les ressources à sa disposition pour éviter un scénario où elle dépense trop ses ressources. D'un autre côté, P3 a déclaré: « Nous trouvons un budget de ce dont nous pensons avoir besoin, comme augmenter le stockage de notre centre de données ou peut-être obtenir de nouveaux serveurs. » Sur la base de cette réponse de P3, les dépenses ne sont planifiées que pour les ressources nécessaires à un moment donné et non pour tous les autres besoins. En d'autres termes, le budget sur ce qu'il faut dépenser priorise d'abord les besoins les plus urgents avant d'envisager d'autres besoins moins urgents. P5 a expliqué qu'ils mettent généralement de l'argent de côté pour le service informatique afin de se prémunir contre toute éventualité découlant d'incidents de cybersécurité. Selon la réponse de P5, cette approche budgétaire reconnaît que l'informatique est un domaine dynamique qui nécessite des plans financiers appropriés bien avant toute éventualité invisible.

Ces réponses des participants à la recherche confirment la position de Fielder et coll. (2016) selon laquelle, en tant que processus, l'acquisition constitue un élément fondamental de la stratégie de cybersécurité, car les organisations doivent se procurer toute la technologie et tous les actifs nécessaires qui faciliteront l'actualisation de leur stratégie. Par exemple, les ressources cloud peuvent faire partie des actifs de base dont une organisation à but non lucratif dépend pour faciliter sa stratégie de cybersécurité

(Bildosola et al., 2015). L'acquisition de telles ressources cloud est nécessaire pour garantir que la stratégie de cybersécurité de l'organisation à but non lucratif devienne une réalité. Les plans d'acquisition devraient être la première étape du processus budgétaire de l'organisation pour assurer un équilibre efficace des ressources (Fielder et coll., 2016). Les organismes sans but lucratif peuvent ne pas avoir la capacité financière adéquate de posséder les actifs de cybersécurité les plus efficaces qui garantissent une stratégie plus fiable en raison de leur confiance dans les dons et les subventions (Jagalur et coll., 2018). La budgétisation aide à planifier les dépenses limitées des ressources en assurant la priorisation des acquisitions les plus nécessaires (Fielder et coll., 2016).

Les réponses des participants et les données probantes tirées des divers documents d'archives concordent avec le concept de la TPS, qui cherche à s'identifier à l'ensemble des problèmes scientifiques et sociaux (Bridgen, 2017). La sécurité et la sûreté des données sont des défis scientifiques et sociaux, qui peuvent être gérés efficacement en intégrant l'éducation scientifique. Lorsque les organismes sans but lucratif planifient leurs ressources pour se procurer les outils et les stratégies informatiques nécessaires pour garantir la sécurité de leurs données et de leur information, ils établissent une systéologie générale qui intègre éventuellement l'éducation scientifique (Drack et Pouvreau, 2015). Essentiellement, l'acquisition est une méthode cruciale qui vise à aborder les domaines non physiques de la science. Ainsi, le concept de LA TPS aide à expliquer comment l'acquisition des outils et des stratégies informatiques appropriés contre le vol de données nous rapproche de l'unité de l'objectif de la science, car elle se développe sur des

principes fonctionnant « verticalement » dans l'univers des sciences distinctes (Bertalanffy, 1968).

Audit

L'audit fait référence à l'évaluation de l'efficacité des mesures de cybersécurité mises en place pour assurer des résultats maximaux. Selon Alkalbani et coll. (2017), une organisation ne peut pas déterminer l'efficacité de ses stratégies de cybersécurité à moins qu'elles ne mesurent le degré de conformité en matière de protection des données. Les réponses des participants sur la question de l'audit ont fait ressortir son importance dans l'ensemble du domaine de la cybersécurité. Trois documents d'archives évalués par le chercheur ont également souligné l'importance de l'audit de cybersécurité de différentes manières. P2 a déclaré: « Nous évaluons les employés et voyons quels domaines nécessitent de les former. » Le document d'archives attribué à l'organisation 2 se lisait en partie comme suit : « Des audits opérationnels, de procédures et de sécurité réguliers aident à s'assurer que des contrôles appropriés sont adéquats pour garantir la confidentialité de l'information, protéger les renseignements personnels identifiables (PII), protéger la disponibilité du système et promouvoir un degré plus élevé d'intégrité des données. » À partir de la réponse de P2 et des données d'archivage de l'Organisation 2, l'entreprise comprend le rôle essentiel que joue l'audit dans le maintien de la cybersécurité. L'organisation a cessé de procéder à des vérifications opérationnelles régulières et à des vérifications de ses employés afin de déterminer les bons programmes de formation.

P1 a souligné l'importance de l'audit de cybersécurité en déclarant: « Nous embauchons une entreprise externe pour venir exécuter un audit sur notre système d'information afin de nous assurer que nous avons tout en place. » Un document d'archives de l'organisation 1 a corroboré la réponse de P1 dans une section de son contenu qui indiquait: « Un audit annuel de cybersécurité par un tiers neutre sera effectué tel que déterminé par l'autorité compétente de l'organisation pour certifier que toutes les directives de sécurité nécessaires sont pleinement respectées. » La réponse de P1 et les éléments de preuve présentés dans le document d'archives montrent clairement que l'organisation entreprend régulièrement des vérifications de cybersécurité par l'entremise d'une entité tierce. P4 a ajouté que son organisation externalise les services d'audit d'entreprises externes, ce qui les aide à évaluer le risque et à identifier leur taux de réussite en ce qui concerne les performances en matière de cybersécurité. Pour P4, la rigueur et le professionnalisme des audits des entreprises externes donnent une image plus précise de la position de l'organisation concernant leurs stratégies de cybersécurité. P3 a déclaré: « Nous manipulons et vérifions les mots de passe d'audit et tout ce qui est important. » Un document d'archives de l'organisation 3 indique que l'entreprise n'attend pas qu'elle soit attaquée. Au lieu de cela, il effectue de manière proactive des audits de cybersécurité pour établir une base de référence de sécurité afin de vérifier les conseils professionnels de l'auditeur. Selon les explications de P2 et même le document d'archives de l'Organisation 2 mentionné, l'audit du système par le biais de manipulations internes délibérées aide à déterminer les faiblesses potentielles qui peuvent nécessiter des mesures urgentes pour faire amende honorable.

Les réponses des participants à la recherche confirment le raisonnement d'Alkalbani et coll. (2017) selon lequel les organisations devraient en effet s'engager à déterminer l'efficacité de leurs stratégies de cybersécurité si elles cherchent véritablement à connaître leur niveau de conformité en matière de protection des données. De plus, ces réponses des participants à la recherche soulignent l'observation de Moskal et coll. (2018) selon laquelle les organisations doivent toujours avoir des processus existants qui offrent des conseils sur les procédures d'amélioration et de gouvernance, ce qui garantit une confiance continue dans les contrôles. Dans la même position, la position de Libicki (2017b) sur les organisations à but non lucratif qui ont besoin d'un système de surveillance et d'intervention pratique pour assurer un mécanisme de réponse en temps réel aux violations est en outre parfaitement liée aux réponses des participants. Alors que les organisations à but non lucratif planifient l'audit de leurs systèmes pour se protéger contre les violations, elles doivent établir des contrôles, des processus et une technologie pour offrir la protection si nécessaire. Cependant, comme Cobb et coll. (2018) l'ont souligné à juste titre, ces contrôles, procédures et technologies anti-violation ne sont pas suffisants pour assurer une sécurité totale. Les ISSM de l'organisation à but non lucratif doivent s'assurer qu'ils évaluent en permanence tous les systèmes et technologies anti-violation pour assurer une fonctionnalité complète.

Le concept de TPS constitue un aspect de philosophie du système, qui s'harmonise efficacement avec la vérification des stratégies de cybersécurité afin d'assurer des résultats optimaux. Les cyberattaques sont incroyablement impliquées dans le sens où certaines des stratégies conçues pour protéger les organisations finissent par

perdre de leur dynamisme au fil du temps (Oakley, 2019). En évaluant continuellement l'efficacité de ces méthodes d'intervention, les organismes sans but lucratif améliorent de plus en plus leur sécurité parce qu'ils peuvent déterminer les méthodes d'intervention les plus efficaces (Cobb et coll., 2018). Sur la base du concept de TPS, les organismes à but non lucratif font appel à des sociétés tierces pour auditer leurs systèmes et déterminer leur efficacité. Les principes fondamentaux de la théorie de la TPS permettent aux organisations de vérifier leurs systèmes au moyen de sous-systèmes offerts par des systèmes tiers comme des fournisseurs externes (Atoum et Otoom, 2016).

Conscience

La sensibilisation à la cybersécurité en tant que sous-thème de cette recherche signifie une compréhension ou une connaissance du concept de cybersécurité et des stratégies de base utilisées pour améliorer la sécurité et la protection des données. En général, la sensibilisation à la cybersécurité constitue l'un des éléments les plus essentiels de la sécurité des données (Bauer et coll., 2017). Les employés constituent le groupe des utilisateurs informatiques d'une organisation, ce qui signifie que leur compréhension de la cybersécurité, en général, aiderait de manière assez significative à garantir la sécurité et la protection des données (Bauer et al., 2017). D'après les réponses des participants, il est clair que la sensibilisation à la cybersécurité a des répercussions positives sur l'état de cybersécurité d'une organisation. Trois documents d'archives ont fourni au chercheur des détails supplémentaires pour effectuer une analyse de recherche sur la sensibilisation à la cybersécurité. P1 a déclaré qu'il est toujours essentiel pour les employés de découvrir et de comprendre leurs événements, en particulier en ce qui concerne les technologies, car

cela intégrerait leur aide pour assurer la sécurité de la cybersécurité. Le document d'archives de l'Organisation 1 indiquait : « En tant que membres de l'organisation, tous les membres du personnel sont responsables et ont le mandat de montrer qu'ils comprennent leur responsabilité exceptionnelle, dans le cadre de la défense visant à protéger les données, les informations et la réputation de l'organisation. » En analysant la réponse de P1 et le contenu du document d'archives de l'organisation 1, il est clair que l'organisation s'attend à ce que ses employés aient des connaissances en cybersécurité et utilisent les mêmes connaissances pour assurer la protection des données.

Selon P4, outre la formation programmée des employés, leur organisation organise une formation de sensibilisation à la sécurité quatre fois par an, dont l'intention est de donner aux employés les moyens de lutter contre les cyberattaques. Le document d'archives de l'organisation 4 indiquait que « le personnel sera suffisamment formé à intervalles réguliers pour lui permettre de protéger les données et les informations de l'organisation contre les pirates et autres acteurs malveillants ». L'examen de la réponse de P4 et du document d'archives de l'organisation 4 informe le fait que l'organisation atteint la sensibilisation à la cybersécurité principalement en formant régulièrement les employés. P5 a déclaré qu'ils organisent même des attaques simulées à l'insu des employés et vérifient leurs niveaux de sensibilisation. Le document d'archives de l'Organisation 5 se lit comme suit : « Dans le cadre de notre politique proactive en matière de cybersécurité, le responsable de la sécurité de l'information effectuera occasionnellement des attaques fictives pour tester l'efficacité des mécanismes de protection des données. » Sur la base de la réponse de P5 et des données d'archivage de

l'organisation 5, ils se concentrent strictement sur la sensibilisation des employés par le biais d'attaques manipulées pour déterminer leur niveau de préparation contre les attaques réelles.

Les réponses des participants à la recherche ci-dessus et les divers éléments de preuve documentés épousent la conclusion de Bauer et coll. (2017) selon laquelle la sensibilisation à la cybersécurité au sein de l'organisation est le meilleur moyen pour les organismes sans but lucratif de motiver le comportement des employés pour freiner les violations de données. En réalité, la plupart des organisations à but non lucratif mettent peu d'efforts pour établir des stratégies de cybersécurité efficaces car elles considèrent qu'il s'agit d'une opération coûteuse par rapport à leurs budgets maigres. Bauer et coll. (2017) ont exposé cette réalité en notant que de nombreux organismes sans but lucratif ne disposent pas de ressources financières adéquates pour acquérir les compétences et l'infrastructure informatiques vitales pour leur utilisation. Cependant, comme Bauer et coll. (2017) l'ont noté, le manque de compétences appropriées en cybersécurité au sein de l'organisation l'expose à des atteintes à la protection des données et à des menaces importantes. Les organisations à but non lucratif doivent maintenir un personnel informatique dédié pendant longtemps pour créer une richesse d'expérience et de compétences qui permettront d'atteindre la sensibilisation interne requise à la cybersécurité. Selon McMahon et al (2015), l'incapacité des organismes à but non lucratif à maintenir un personnel informatique dédié prive l'organisation de la sensibilisation nécessaire qui améliorerait la protection contre les pirates et les violations de données en général. Le manque de sensibilisation dans les organisations à but non

lucratif a également entraîné l'utilisation courante de logiciels open source pour réduire les coûts. Selon Bauer et coll. (2017), l'utilisation du logiciel open source augmente la vulnérabilité aux cyberattaques contrairement à l'utilisation de versions logicielles propriétaires.

Les réponses et les preuves de documents d'archives font également écho à l'observation d'Almubark et coll. (2016) selon laquelle la sensibilisation est une stratégie efficace qui fonctionne en créant une culture de sécurité influente, qui tient toujours les employés au courant de la technologie, notamment en leur permettant de comprendre les processus ainsi que d'autres facteurs organisationnels qui touchent à la sécurité des données.

D'après les réponses des participants et les documents à l'appui, la sensibilisation à la cybersécurité est fortement liée à la TPS, car elle assure un système pratique contre le vol ou la manipulation de données. En particulier, la TPS considère une organisation comme un système ouvert en interaction constante avec son environnement local grâce à l'échange de « matériaux » (Schneider et coll., 2016). Essentiellement, lorsque les organisations créent une forte sensibilisation à la cybersécurité parmi les employés, elles recherchent un mécanisme destiné à sécuriser continuellement l'organisation même si elle interagit continuellement avec son environnement local. Les cyberattaques augmentent lorsque l'organisation ne parvient pas à rationaliser et à harmoniser ses politiques, ses logiciels, son matériel et sa formation.

Plan de sécurité

Un plan de sécurité fait référence à la stratégie globale d'une organisation visant à protéger ses clients, ses employés et ses informations d'entreprise contre toute compromission. Les participants ont répondu en décrivant certains des plans de sécurité de leur organisation, soulignant leur importance en ce qui concerne la stratégie de cybersécurité. Sept documents d'archives analysés par le chercheur ont fourni le terrain supplémentaire pour élaborer sur l'essence des plans de cybersécurité en général. P1 a déclaré: « Nous devons investir beaucoup plus dans la sécurité des données en termes d'avoir plus d'outils à notre disposition pour rester un peu plus proactif. Nous utilisons notre système antivirus et notre système de protection contre les intrusions pour nous assurer que nous sommes toujours prêts à faire face à toute sorte de violation de données ou d'attaque. Le document d'archives de l'organisation 1 indiquait : « Le responsable informatique détermine l'adoption d'un logiciel antivirus et d'outils de protection contre les logiciels malveillants supplémentaires pour détecter, prévenir, dissuader et atténuer l'introduction et l'exposition de virus/logiciels malveillants sur les périphériques informatiques et les réseaux au sein de l'organisation. » La réponse de P1 et le document d'archives de l'Organisation 1 mettent en évidence les antivirus et d'autres outils connexes tels que les systèmes de protection contre les intrusions dans le cadre des plans de sécurité contre les cyberattaques.

P2 a déclaré: « Le contrôle d'accès est un grand, et nous sommes là pour parler d'authentification pour chaque individu touchant n'importe quel système et toutes les ressources d'information. Les employés dans des environnements distants ont besoin d'une authentification à deux facteurs. Cette réponse de P2 identifie la façon dont les

organisations limitent l'accès à leurs systèmes et réseaux de données comme une stratégie pour limiter la compromission par les pirates et autres personnes non autorisées. P3 a décrit les plans de sécurité de leur organisation, en se concentrant davantage sur les individus, car chaque employé couvre un aspect de sécurité spécifique dans ses domaines de niche. L'organisation n'a pas de contrôle centralisé et compte plutôt sur les employés comme plan de sécurité principal. Les données d'archivage de P3 ont déclaré: « Cette politique approuve les services cloud pour nécessiter le partage et le stockage de fichiers 1) avec des fournisseurs fournissant une protection et une récupération appropriées pour les informations de l'organisation, et 2) avec des restrictions claires sur le stockage des informations protégées de l'organisation. » Sur la base des réponses de P3 et du document d'archives de l'Organisation 3, les organisations ont recours au stockage de données à l'externe dans le cadre de leurs plans de sécurité pour se protéger contre les pertes et les compromissions de données.

P4 a parlé d'un plan de sécurité dans lequel une entreprise tierce collecte toutes les données au format numérique et les désinfecte pour assurer une normalisation appropriée et périodique de tout. Le document d'archives de l'organisation 4 a déclaré: « L'organisation fournira à tous les membres du personnel l'accès à Microsoft Office 365 et Google Apps. Les membres du personnel accéderont à Microsoft « OneDrive Entreprise » et « Google Drive » à l'aide de comptes créés sur leur ID de connexion. La réponse de P4 et les preuves contenues dans le document d'archives de l'Organisation 4 montrent également comment les organisations ont recours à des acteurs tiers dans le cadre de leurs plans de sécurité des données.

Les réponses de ces participants à la recherche concordent avec les observations de Martin et Murphy (2017) selon lesquelles les organisations doivent renforcer à l'avance une capacité adéquate pour protéger leurs renseignements de nature délicate. Les organisations à but non lucratif peuvent trouver la confidentialité des données plus difficile à mettre en œuvre en raison de la fluidité du concept par rapport à leurs capacités marginales, mais la réalité souligne la nécessité pour les organisations de protéger leurs données et leur infrastructure informatique contre les compromissions des pirates. Selon Adams (2017), la planification de la sécurité des données aide les organismes sans but lucratif à définir clairement la confidentialité des données et à établir efficacement des mécanismes pour y remédier. La planification de la cybersécurité qui comprend les systèmes antivirus, les stratégies de protection contre les intrusions et l'informatique en nuage constitue de meilleurs systèmes organisationnels soulignés par la TPS (Zhang et coll., 2019). En particulier, les organisations à but non lucratif doivent s'efforcer de créer un mécanisme de protection pour leurs données et leurs actifs informatiques bien à l'avance afin d'assurer la proactivité lorsqu'il s'agit de protéger les données sensibles à leur disposition (Abouelmehdi et al., 2017). La planification de la sécurité des données au niveau des organismes à but non lucratif, selon Adams (2017), cible l'enracinement du stockage et les processus de transport dans le cadre des mesures de sécurité.

En général, les réponses des participants à la recherche et les preuves documentaires tirées des organisations ont souligné le lien entre la planification de la cybersécurité et le concept de TPS. Selon Proctor et Xiong (2018), les principes de la TPS sont liés aux principes de la cybernétique en ce sens que tout ce qui commence, des

systèmes neurophysiologiques aux activités sociétales, peut être transformé en systèmes de contrôle structurés constituant des boucles de rétroaction et de rétroaction. Lorsque les organisations planifient la cybersécurité, elles élaborent des stratégies au moyen d'inférences scientifiques qui résument la prise de décision humaine en fonction des résultats d'expériences contrôlées (Proctor et Xiong, 2018). De nombreuses organisations font face à la pression des progrès technologiques dans un système où les vies humaines sont de plus en plus étroitement liées au cyberespace. En raison de l'interaction accrue, les organisations estiment qu'il est nécessaire de poursuivre la psychologie cognitive et la recherche interdisciplinaire dans le cadre de leur planification de la sécurité (Proctor et Xiong, 2018). La nature complexe des cyberattaques nécessite une approche différente des défenses de sécurité. Les menaces dynamiques de la nouvelle génération sont évasives, résilientes et complexes, ce qui nécessite une planification appropriée pour lutter contre les menaces. Les organisations à but non lucratif doivent collecter et partager des informations en temps réel sur les cybermenaces pour les convertir en informations précises sur les menaces afin de prévenir les attaques ou de mettre en œuvre une reprise après sinistre en temps opportun. Ainsi, le lien entre la planification de la cybersécurité et la TPS fournit les outils qui se concentrent sur la lutte contre le cycle cybernétique (De Boer et Andersen, 2016). Selon Fal (2016), la planification de la sécurité en cybersécurité est une forme de mécanismes de rétroaction en boucle fermée dont la sortie est directement liée à l'entrée du système ultérieur. La TPS constitue des boucles de rétroaction utilisant des relations comportementales (Drack et Pouvreau, 2015).

Procédures de sécurité

Les procédures de sécurité font référence à l'ensemble de règles qu'une organisation établit sur la pratique de la sécurité responsable pour guider les employés, les partenaires, les membres du conseil d'administration, les consultants et les autres utilisateurs finaux accédant aux ressources Internet et aux applications en ligne, en envoyant des données sur les réseaux. Sur la base des réponses des participants, des procédures de sécurité existent dans leurs organisations dans le cadre de leur stratégie de cybersécurité élaborée. Cinq documents d'archives étaient disponibles au cours de l'analyse de cette recherche. En tant que pratique courante, la plupart des organisations adhèrent à un ensemble de pratiques et de processus de sécurité pour s'assurer que leurs données restent en sécurité en tout temps (Gordon et coll., 2015). P5 a noté: « L'une des procédures que nous utilisons comprend le contrôle d'accès, où nous nous assurons que l'accès au système reste limité aux personnes censées utiliser les actifs. » Un document d'archives de l'Organisation 5 indiquait que « les ID de groupe ne sont généralement pas autorisés comme moyen d'accès aux données de l'organisation, mais peuvent être approuvés dans des situations exceptionnelles si d'autres contrôles d'accès adéquats sont en place ». Cette réponse de P5 et les preuves corroborantes du document d'archives de l'organisation 5 identifient la façon dont les organisations s'engagent à utiliser le contrôle d'accès dans le cadre de leurs procédures de cybersécurité.

P1 a déclaré qu'une partie de ses procédures comprenait l'utilisation d'un système antivirus, d'un système de protection contre les intrusions et l'obligation pour les utilisateurs de changer leur mot de passe tous les 60 jours. Les utilisateurs sont également tenus d'utiliser un mot de passe complexe contenant des caractères spéciaux, des

nombres et des uppercuts inférieurs. Un document d'archives de l'organisation 1 indiquait : « Les utilisateurs doivent recevoir une formation sur la protection par mot de passe, la politique de mot de passe étant mise en œuvre pour confirmer que les utilisateurs changent leur mot de passe tous les 60 jours ou selon ce qui doit être déterminé par le gestionnaire de la sécurité de l'information. » Les preuves mentionnées dans la réponse de P1 et le document d'archives de l'Organisation 1 révèlent que les organisations peuvent utiliser une combinaison de stratégies, y compris des politiques de mot de passe strictes, des systèmes antivirus et des mécanismes de protection contre les intrusions, dans le cadre de leurs procédures de cybersécurité. P2 a ajouté: « Pour accéder au système, certains ne peuvent lire que toutes les informations tandis que d'autres ne peuvent lire que certaines informations. Certains peuvent lire et écrire dans le système et même modifier les données dans le système, qui font toutes partie de nos procédures de sécurité. Le document d'archives de l'Organisation 2 indiquait ce qui suit : « Les employés ne peuvent accéder qu'à l'information nécessaire à l'exécution efficace de leurs tâches respectives. L'accès sera basé sur la responsabilité ou la compétence professionnelle d'un employé, son accès aux ressources de données se limite à la visualisation, à la création ou à la modification de fichiers. La réponse de P2 et les détails dans le document d'archives de l'Organisation 2 indiquent que le contrôle d'accès basé sur les rôles fait partie des procédures de cybersécurité que les organisations utilisent pour protéger leurs données contre la compromission et le vol.

P3 a expliqué que l'organisation dispose d'un paramètre de sensibilité, qui protège les informations sensibles envoyées via Internet avec des fonctionnalités telles

que l'expiration du mot de passe d'une semaine. Ces informations sensibles se suppriment automatiquement si le mot de passe expire dans le délai imparti. Les données d'archivage attribuées à l'organisation 3 ont enregistré : « Les données sensibles seront automatiquement supprimées du stockage ou du périphérique informatique qui les contient immédiatement après l'expiration du mot de passe utilisé pour les protéger. » Sur la base de cette réponse de P3 et des preuves de données d'archivage, il est clair que les organisations utilisent des systèmes automatiques qui peuvent auto-supprimer toutes les données considérées comme sensibles pour les protéger des pirates et autres acteurs malveillants. P4 a répondu que les procédures de sécurité de leur organisation vont de la mise en œuvre d'une stratégie de groupe à un logiciel appelé applications serveur qui gèrent les utilisateurs privilégiés et suivent les appareils de point de terminaison. La réponse de P4 souligne l'utilisation de comptes d'utilisateurs privilégiés par les organisations dans le cadre de leurs procédures de cybersécurité qui n'autorisent que des niveaux d'accès spécialisés basés sur des niveaux d'autorisation élevés.

Ces réponses des participants à la recherche soulignent la position de Gordon et coll. (2015) selon laquelle, en général, de nombreuses organisations adhèrent à la pratique courante d'observation des pratiques et des processus de sécurité comme moyen de garantir la sécurité en tout temps. De même, les réponses font écho aux conclusions de Bauer et coll. (2017), qui postulaient que les organismes sans but lucratif s'engagent dans de nombreuses procédures de sécurité telles que la sensibilisation aux systèmes d'information par le biais de programmes spéciaux mis en œuvre par les gestionnaires des SI. Almubark et coll. (2016) ont observé que le besoin des organismes sans but

lucratif de créer une culture de sécurité influente dans le cadre de leur procédure de sécurité est également en tandem avec les réponses des participants à la recherche. Selon Almubark et al., une telle culture de sécurité dans l'organisation à but non lucratif peut atteindre l'objectif visé en motivant le comportement des employés pour freiner les violations de données. De même, les réponses des participants à la recherche confirment Zafar et coll. (2016) selon lesquelles les organisations doivent mobiliser le soutien de la haute direction pour les pratiques de gouvernance des TI afin d'assurer des procédures de sécurité adéquates.

En général, le concept de procédures de sécurité dans les organismes sans but lucratif est lié à la philosophie du système adoptée par la TPS. En particulier, la philosophie du système vise à développer une nouvelle pensée ou un nouveau point de vue basé sur des concepts de systèmes. Ainsi, les organismes sans but lucratif comprennent des systèmes ouverts caractérisés par des contingences qui font face à des conséquences importantes lorsqu'ils sont confrontés à des violations de données (Caws, 2015). Les principaux composants d'un système à but non lucratif sont les entrées, les sorties, les processus, les sous-systèmes et les commentaires. En établissant des procédures de sécurité efficaces, les organismes sans but lucratif peuvent identifier les symptômes des atteintes à la cybersécurité et les décrire de manière indépendante et comment ils interagissent pour aider à comprendre comment l'organisation peut les prévenir (Rousseau, 2015).

Formation

La formation fait référence à l'enseignement intentionnel des individus de l'organisation à transmettre des compétences qui renforceraient leurs efforts de protection des données et de l'information. Les réponses des participants portaient sur la formation concernant leurs stratégies respectives en matière de cybersécurité. De plus, les documents d'archives consultés par le chercheur ont corroboré les réponses des participants de manière assez spectaculaire. La formation des employés à la cybersécurité confère des compétences pour améliorer la sécurité globale de l'organisation, réduire les erreurs évitables qui peuvent causer des pertes et des violations de données, améliorer la réputation de l'entreprise et renforcer la confiance des employés (Almubark et coll., 2016). Lorsque les employés reçoivent une formation adéquate en cybersécurité et en sécurité, l'organisation augmente sa productivité et minimise ses coûts d'exploitation (He et Zhang, 2019). P1 a déclaré : « Nous nous assurons d'éduquer nos utilisateurs sur ce qu'ils devraient faire. » Le document de politique de l'organisation 1 indiquait ce qui suit : « Tous les employés de l'organisation ayant accès aux ressources d'information doivent suivre une formation de sensibilisation à la sécurité dans les 30 premiers jours suivant leur embauche. » D'après la réponse de P1 et le document de politique de l'Organisation 1, il est évident que les organisations utilisent la formation obligatoire sur la cybersécurité dans le cadre de leurs stratégies pour doter leur personnel de connaissances sur la protection et la sécurité des données.

P2 a répondu : « Nous avons des sessions de formation avec les utilisateurs où ils peuvent poser des questions. » Sur la base de cette réponse de P2, il est évident que les organisations insistent sur la nécessité de former régulièrement leurs employés pour créer

une base de connaissances interne importante qui aiderait à se prémunir contre le vol et la compromission des données. P3 a déclaré : « Nous formons nos employés. La formation est importante, et elle n'a pas besoin d'être formelle parce que nous avons des experts qui le font au jour le jour. Cela pourrait être une chose simple comme une conversation de 15 à 20 minutes. Le document de politique de l'organisation 4 indiquait : « L'organisation doit continuellement évaluer les compétences en cybersécurité détenues par tous les employés et promouvoir une formation régulière pour combler toute lacune potentielle en matière de compétences. » L'analyse de la réponse de P3 et des détails dans le document d'archives de l'organisation 4 révèle comment les organisations investissent plus de temps et de ressources pour investir dans des programmes de formation afin de faire face efficacement aux menaces à la cybersécurité. P4 a expliqué que son organisation utilise deux stratégies : envoyer les employés à la formation et mener une formation interne pour les personnes du service de sécurité informatique. Selon P4, la formation externe a lieu au moins une fois par mois, où une personne de l'équipe reçoit les compétences nécessaires. Sur la base de la réponse de P4, les organisations adoptent également une combinaison de méthodologies de formation pour s'assurer que leurs stratégies de cybersécurité sont suffisamment convaincantes.

La création d'une solide culture de sécurité des données constitue une approche appropriée que les organismes sans but lucratif peuvent adopter pour réaliser efficacement la cybersécurité (Zafar et al., 2016). La formation des employés sur la cybersécurité utilise éventuellement des programmes spéciaux impliquant des interventions planifiées systématiques qui informent sans interruption les employés et les

intervenants sur les informations de sécurité (Bauer et al., 2017). La formation crée une sensibilisation à la culture en motivant les employés à développer des comportements pour freiner les atteintes à la protection des données (Almubark et coll., (2016). La formation est une stratégie efficace pour créer une culture de sécurité influente, car elle garantit que les employés sont continuellement mis à jour sur la technologie. La formation permet également aux employés de comprendre les facteurs organisationnels et d'autres processus importants concernant la sécurité des données (Almubark et coll., 2016). Selon Zafar et al., la formation des employés ne construit pas seulement une culture de sécurité des données convaincante, mais améliore également les activités de gestion des risques et la planification de la sécurité.

La formation en cybersécurité est un concept essentiel étroitement associé à la TPS. Selon Verhoeff et coll. (2018), la TPS comporte trois aspects : la science des systèmes, la technologie des systèmes et la philosophie des systèmes. La philosophie principale de la TPS est axée sur la façon dont le système fonctionne ensemble et sur la façon dont une partie du système permet de comprendre les autres parties. Dans le cadre du système d'organisation, la formation des employés transmet des idées mathématiques simples qui formulent fondamentalement la rétroaction, l'équilibre, l'information, la stabilité, l'entropie, la réglementation, les contraintes, la communication, etc. La formation sert de mécanisme d'entrée qui interagit avec le système en transmettant continuellement des compétences qui améliorent la volonté des employés de protéger les données (Doherty et Tajuddin, 2018). Selon Kim et Kim (2017), l'utilisation de la formation comme mécanisme d'interaction avec le mécanisme de cybersécurité permet

d'atteindre le comportement de conformité approprié grâce à la culture matérielle et à l'infrastructure de soutien. Les organismes sans but lucratif ont le devoir de promouvoir la conformité en intégrant une formation critique pour encourager les employés à faire des efforts volontaires. Lorsque les organisations à but non lucratif forment leurs employés pour améliorer leurs connaissances en cybersécurité, elles leur permettent d'obtenir de meilleures connaissances en matière de science des systèmes, de technologie des systèmes et de philosophie des systèmes, qui se combinent pour assurer une organisation sûre en termes de sécurité des données.

Thème 3 : Dépendance à l'égard de tiers

Les sous-thèmes de ce thème comprennent le soutien technique d'experts, la limitation des responsabilités des organismes à but non lucratif et la limitation de l'exposition au risque. L'intégration du support tiers est un moyen efficace de mettre en œuvre la cybersécurité, en particulier pour les organisations à but non lucratif qui manquent d'expertise informatique interne critique (Rossouw &Willett, 2017). Le tableau 4 met en évidence les sous-thèmes de la dépendance à l'égard de thèmes de tiers.

Tableau 4

Sous-thèmes sous la dépendance à l'égard du tiers

	Participants		Documents	
Thèmes majeurs/mineurs	Compter	Références	Compter	Références
Support technique d'experts	5	20	4	13
Limitation des passifs sans but lucratif	5	3	2	9
Limiter l'exposition au risque	5	5	2	3

Support technique expert

Le support technique expert fait référence à l'aide ou à l'assistance de réserve que les spécialistes de la cybersécurité utilisent souvent auprès des utilisateurs de systèmes informatiques et de réseaux de données pour renforcer leurs efforts contre les menaces et les risques liés aux données. La plupart du temps, les entreprises informatiques tierces apportent leur support technique qui profite souvent aux organisations clientes qui n'ont pas le même niveau de capacité(Jagalur et al., 2018). L'efficacité opérationnelle des sociétés informatiques tierces garantit aux organisations clientes un avantage absolu en termes de coûts en raison de leur main-d'œuvre expérimentée, de leur matériel élaboré et de leurs ressources logicielles construites au fil du temps(Gordon, Loeb et al., 2015). Les réponses des participants ont indiqué que leur organisation dépendait de fournisseurs de services de TI tiers pour des raisons de soutien technique. De même, les documents d'archives évalués dans le cadre de cette étude ont souligné l'importance des fournisseurs tiers dans l'offre d'un soutien technique en matière de cybersécurité. P4 a postulé: « Le fournisseur fait ce qu'il fait toute la journée parce qu'il est spécialisé, qu'il a les compétences et qu'il a les ressources nécessaires pour protéger. » Le document de politique de l'Organization 4 indiquait que l'organisation ferait appel à des spécialistes et à des fournisseurs tiers en TI chaque fois que cela serait nécessaire pour offrir un soutien technique tel qu'il serait déterminé. Une analyse de la réponse ci-dessus par P4 et du contenu du document de politique montre que les organisations s'appuient souvent sur des sociétés informatiques tierces pour un support technique expert afin d'appliquer leurs mécanismes de sécurité contre la perte et la compromission des données.

P2 a déclaré qu'elle avait confié à un fournisseur de services infonuagés la gestion de toutes les opérations en son nom afin de concentrer les activités de ses clients. Le document d'archives d'Organization 2 indiquait : « Le fournisseur de services cloud externe doit étendre les services de support aux utilisateurs chaque fois que cela est nécessaire. » Sur la base de la réponse de P2 et des preuves contenues dans les données d'archivage d'Organization 2, il est déductible que les organisations utilisant des services cloud bénéficient également d'un support technique qui les aide dans leur quête pour assurer la sécurité de leurs données et informations. P5 a expliqué que son organisation dépend d'un système de fournisseur qui gère tous ses besoins informatiques qu'il juge trop technique pour gérer. La réponse de P5 souligne le fait que les organisations reçoivent une combinaison de soutien technique de fournisseurs de services externes pour combler leur manque d'insuffisances en matière de cybersécurité.

Les réponses de ces participants à la recherche concordent avec les conclusions de Bauer et coll. (2017) selon lesquelles la plupart des organismes sans but lucratif ont intégré de nombreuses procédures de sécurité qui impliquent l'intégration d'opérations de tiers. Compte tenu de la capacité limitée en matière de TI et de compétences dans la plupart des organismes sans but lucratif, la possibilité d'obtenir un soutien technique auprès de fournisseurs de services tiers garantit une performance efficace en matière de cybersécurité (Jagalur et coll., 2018). Selon Gordon et coll. (2015), les fournisseurs de services de TI tiers garantissent aux organisations clientes l'efficacité opérationnelle en termes de coût et de qualité de rendement. Le support technique expert des acteurs tiers garantit une fabrication efficace, des ressources logicielles de haut niveau et du matériel

élaboré acquis au fil du temps(Gordon, Loeb et al., 2015). Les réponses des participants à la recherche englobent également le point de Bauer et al. selon lequel les fournisseurs tiers de confiance constituent des mesures d'intervention critiques adaptées aux ISSM des organismes à but non lucratif pour la gestion de la sécurité. Néanmoins, les organisations à but non lucratif doivent comprendre les rôles et les capacités attribués à des fournisseurs tiers spécifiques avant de faire appel à leurs services pour obtenir un support technique expert.

Le soutien technique d'experts constitue un aspect essentiel de la TPS. Selon Ludwig von Bertalanffy (1968), un système atteint un fonctionnement sain lorsque ses parties s'interdépendant avec succès les unes des autres. Une caractéristique marquante de cette définition est l'interdépendance des parties au sein d'un système. Ainsi, dans un contexte organisationnel, le soutien technique d'experts peut être considéré comme un élément important de la réalisation du fonctionnement sain de l'organisation (Bridgen, 2017). Le processus principal qui caractérise la façon dont les composants se rapportent dans un système est la propension homéostatique qui lisse ou équilibre les opérations. Le support technique expert au sein de l'organisation aide à lisser les opérations, ce qui garantit le bon fonctionnement de l'organisation dans son ensemble.

Limitation des responsabilités des organismes sans but lucratif

Sur la base de l'analyse des données, les organisations à but non lucratif envisagent de limiter leurs responsabilités à but non lucratif car elles fonctionnent souvent avec des ressources financières limitées qui entravent leur pleine capacité potentielle. La limitation des responsabilités des organismes sans but lucratif fait

référence à la pratique des organisations visant à minimiser l'obligation de pertes de données et de compromission par les pirates (Jagalur et al., 2018). La réponse de P1 a capturé les mêmes sentiments et automatisé des tâches spécifiques pour prévenir les violations de données. Un document d'archives de l'Organisation 1 a corroboré la réponse de P1 indiquant que l'automatisation des opérations à différents niveaux sera priorisée pour limiter l'interaction humaine, augmentant ainsi le risque de perte de données. P3 a laissé entendre que leur organisation a des responsabilités limitées en sous-traitant des services de destruction de données à une entreprise tierce qui le fait efficacement parce que c'est leur principal secteur d'activité. Sur la base de la réponse de P3, les organisations qui n'ont pas de capacité interne font souvent l'acquisition de sociétés spécialisées tierces pour gérer des opérations délicates susceptibles d'entraîner des pertes de données si elles devaient être traitées en interne. P4, d'autre part, a déclaré: « Nous effectuons régulièrement des tests de vulnérabilité sur nos systèmes de données pour nous assurer d'éliminer les faiblesses probables. Les tests sont très variés, allant de l'évaluation des forces et de l'efficacité des mots de passe à l'évaluation des remèdes aux attaques DDoS mis en œuvre.

Sur la base des réponses des participants à la recherche, il existe un lien entre les idées mentionnées et la littérature d'Alshahrani et Traore (2019), postulant que les protocoles de sécurité automatisés mettent en œuvre de nombreux mécanismes d'analyse de sécurité programmés. La robustesse de ces systèmes automatisés peut aider efficacement les organisations à but non lucratif à suivre, détecter et éliminer les menaces de cybersécurité par rapport aux systèmes manuels gérés par les employés. De même, les

réponses des participants concordent avec les conclusions de Jagalur et coll. (2018) selon lesquelles les fournisseurs tiers protègent considérablement les organisations, y compris les organismes à but non lucratif, contre des passifs trop coûteux et techniques liés aux opérations informatiques. Selon Holtfreter et Harrington (2015), les fournisseurs informatiques tiers se spécialisent dans des domaines informatiques particuliers, ce qui leur donne la plus grande capacité et le potentiel pour gérer les obligations que les organisations clientes telles que les organisations à but non lucratif peuvent ne pas gérer efficacement. Essentiellement, les organisations à but non lucratif transfèrent leurs obligations à un acteur tiers supérieur ayant la capacité adéquate de les protéger contre les responsabilités probables en matière de violation de données.

Le fondement théorique de la TPS s'harmonise avec la discussion concernant la limitation des obligations des organismes sans but lucratif, comme il a été souligné ci-dessus. En particulier, l'organisation est un système ouvert avec une interaction continue avec son environnement local en échangeant des « matériaux »(Schneider et al., 2016). La TPS est une théorie sociale expliquant le partage d'idées, d'arguments, d'hypothèses, de spéculations explicatives et d'expériences de pensée au profit des sociétés et des éléments humains. Les organisations à but non lucratif représentent des sociétés humaines dans lesquelles les interactions sociales se produisent continuellement pour aider à atteindre la cybersécurité. Lorsque les organisations à but non lucratif recherchent des conseils d'experts en cybersécurité, par exemple, elles acquièrent des idées et une expertise qui les aident à atteindre une cybersécurité efficace. L'aspect social de la TPS est utile pour limiter les responsabilités des organismes sans but lucratif, car il favorise le

partage d'idées et de connaissances utiles dont l'adoption et la mise en œuvre protègent contre l'exploitation des données. L'interaction entre l'organisation et les systèmes sociaux appelle les organisations à but non lucratif à limiter les responsabilités potentielles pour garantir des systèmes supérieurs protégés contre les pirates.

Limiter l'exposition au risque

La limitation de l'exposition aux risques aide également les organisations à gérer les cyber risques. Les interventions courantes visant à limiter l'exposition au risque comprennent un examen de sécurité physique de pointe 24 heures sur 24, des contrôles d'accès physique, ainsi qu'une protection périmétrique à plusieurs niveaux (Kajiyama et coll., 2017). Les réponses des participants ont montré qu'ils étaient conscients que leurs organisations à but non lucratif étaient vulnérables aux incidents de cybersécurité et qu'elles s'attaquaient au risque en dépendant des fournisseurs pour fournir l'infrastructure requise. Par exemple, P1 a soutenu que l'organisation surveille de près les identifiants de connexion des employés pour éviter un scénario où les pirates peuvent voler ces informations d'identification et accéder aux bases de données organisationnelles critiques sans être détectés. Le document d'archives de l'organisation 1 indiquait que les employés ne sont pas autorisés à recycler les mots de passe après leur expiration. Les employés sont également censés utiliser leurs données biométriques pour limiter l'exposition aux risques liés aux données dans le cadre de leurs informations de connexion. D'après la réponse de P1 et les éléments de preuve présentés dans le document d'archives de l'Organisation 1, il est évident que l'organisation est proactive dans la mise en place de mesures de sûreté et de sécurité des données pour de bon.

P2 a répondu : « L'organisation a installé des caméras de sécurité à tous les endroits stratégiques pour capturer physiquement des images et des séquences de toute personne, qu'il s'agisse d'employés ou d'étrangers, qui pourrait s'engager dans des activités de violation de données. Le document d'archives de l'organisation 2 indique en partie que les locaux de l'organisation doivent demeurer sous surveillance par caméra de sécurité en tout temps pour aider à détecter les activités qui pourraient compromettre la sécurité de l'information. P3, d'autre part, a répondu : « L'accès à la salle de données de l'organisation est physiquement protégé par une grande porte physique qui ne peut être ouverte qu'à l'aide d'une carte de sécurité délivrée à quelques membres du personnel informatique. Cette intervention a été mise en place pour protéger les données et les systèmes connexes contre la compromission par des intrus. P4 a indiqué qu'en plus du fait que l'organisation bénéficie d'une clôture d'enceinte et d'un agent de sécurité autour de ses locaux, la vidéosurveillance offerte par un réseau de caméras de vidéosurveillance limite considérablement leur exposition à la sécurité. La réponse de P4 souligne l'accent total mis par l'organisation sur l'utilisation d'interventions physiques et non physiques pour limiter l'exposition de ses données aux risques d'exposition. P5 a également mentionné un mécanisme mis en œuvre dans l'organisation où les identifiants de connexion des employés étaient étroitement surveillés et automatiquement annulés après tous les deux mois pour s'assurer que les pirates qui pourraient les voler se voient refuser l'accès au système.

Les réponses correspondent aux observations de la littérature de Kajiyama et coll. (2017) selon lesquelles de nombreuses organisations utilisent un examen de sécurité

physique de pointe 24 heures sur 24, ainsi que des contrôles d'accès physique et une protection périmétrique à plusieurs niveaux pour suivre les actions des pirates. La limitation de l'exposition aux risques aide également les organisations à gérer les cyberrisques. Les organismes sans but lucratif peuvent envisager des interventions telles que des contrôles d'accès physiques, une protection périmétrique à plusieurs couches, etc., pour réduire l'exposition au risque à laquelle ils sont confrontés (Kajiyama et coll., 2017). Les organismes sans but lucratif peuvent également exploiter les systèmes cloud plus robustes qui se concentrent sur la réalisation de la cybersécurité en établissant une infrastructure sur site (Rossouw &Willett, 2017). Étant donné que la plupart des organismes sans but lucratif ne disposent pas de ressources adéquates pour protéger leurs données et leur infrastructure contre les violations, les systèmes cloud leur présentent une alternative pratique qui garantit la sécurité des données sans nécessiter d'investissement initial substantiel (Attaran, 2017). De même, les réponses des participants font écho à Parks et coll. (2017). Ils soutiennent qu'une simple politique de confidentialité sans instituer de mécanismes de protection physique peut s'avérer pratiquement dénuée de sens et très superficielle pour une organisation à but non lucratif. Ainsi, les ISSM dans les organisations à but non lucratif doivent s'efforcer d'utiliser des barricades physiques et d'autres mécanismes de dissuasion pour limiter le risque d'exposition à leurs données et systèmes de données.

Ces réponses des participants à la recherche et les documents d'archives corroborés sont conformes au principe de base de la TPS. En général, l'aperçu d'une stratégie de cybersécurité par GST est du point de vue de l'intégration des systèmes,

soulignant la nécessité pour les organisations de mettre en œuvre une combinaison de stratégies de sécurité des données (Kordova et coll., 2018). Une stratégie de sécurité que les organisations à but non lucratif peuvent mettre en œuvre pour atteindre la cybersécurité comprend la formation des employés. La formation est un aspect de la TPS qui vise à sensibiliser efficacement les employés à l'importance de leur gestion de la cybersécurité (Doherty et Tajuddin, 2018). Les employés informés limiteront l'exposition au risque de l'organisation, car la formation qu'ils suivent renforce leur volonté de protéger les données. Les organisations à but non lucratif bénéficieront d'une protection et d'un contrôle améliorés de la cybersécurité si elles forment leurs employés à atteindre un comportement de conformité de haut niveau. Lorsque les organisations à but non lucratif limitent leur exposition au risque contre la perte de données, elles renforcent leur volonté de prendre les mesures nécessaires pour protéger les données. Les organisations à but non lucratif se lancent dans la promotion des systèmes de conformité pour assurer activement la protection contre les intrusions et le vol.

Applications à la pratique professionnelle

Les résultats de cette étude, les résultats de l'analyse du cadre conceptuel et la revue de la littérature savante contribuent à discuter des stratégies que les ISSM des organismes à but non lucratif utilisent pour se protéger contre les cyberattaques. En particulier, les résultats de l'étude montrent que l'identification de l'exécution par les ISSM des meilleures pratiques de cybersécurité pour protéger l'organisation est la contribution la plus importante. Bordoff et coll. (2017) ont souligné la nécessité pour les

organismes sans but lucratif de former leur personnel à la sécurité et de justifier les pratiques exemplaires des tiers.

Sur la base des résultats de l'étude de recherche, mes résultats illustrent que les ISSM réussis dans les organisations à but non lucratif devraient utiliser efficacement trois stratégies efficaces pour protéger leurs organisations contre les cyberattaques. Le plus souvent, les ISSM dans les organisations à but non lucratif devraient utiliser une stratégie de cybersécurité complète comme technique préférée pour atténuer les menaces de cybersécurité et les violations de données. Les plans stratégiques efficaces impliquaient a) la mise en place d'un plan sur la cybersécurité, b) la protection de l'accès au système à l'aide d'un mot de passe, c) la sensibilisation à la cybersécurité, d) la mise en œuvre de procédures de sécurité et e) la formation. L'essence du plan stratégique est de jeter les bases de l'établissement d'opérations commerciales sécurisées.

Deuxièmement, le succès de l'ISSM dans les organisations à but non lucratif devrait créer une sensibilisation à la cybersécurité en tant que stratégie pour assurer la protection de la cybersécurité. Almubark et coll. (2016) ont souligné le besoin de formation et d'éducation pour accroître les connaissances et la compréhension des employés concernant les risques et leur devoir de protéger les biens d'infrastructure. Les interventions efficaces en matière de sensibilisation à la cybersécurité devraient comprendre a) la compréhension de la protection, b) la compréhension des fournisseurs tiers et c) la compréhension des plans stratégiques. D'après l'analyse des données, il était évident que chacun des ISSM qui ont participé à cette étude corroboré Almubark et coll.,

confirmant que la sensibilisation à la cybersécurité était un élément essentiel d'une stratégie de cybersécurité efficace.

Troisièmement, les ISSM qui ont participé à l'étude ont signalé que les organisations à but non lucratif préfèrent dépendre de fournisseurs tiers comme stratégie pour assurer la protection de la cybersécurité. À partir de l'analyse des données effectuée, j'ai établi que les organisations à but non lucratif n'ont pas suffisamment de compétences, de connaissances et de capacités internes en matière de cybersécurité, ce qui crée la nécessité de s'appuyer sur des fournisseurs tiers de confiance. Chacun des ISSM de cette étude a admis dépendre de fournisseurs tiers pour offrir des services de protection contre les cyberattaques à leurs organisations. Les plans stratégiques les plus efficaces pour les professionnels de l'informatique sont les suivants : (a) employer des opérateurs sûrs et fiables, (b) limiter les responsabilités des ISSM, (c) limiter l'exposition au risque et (d) tirer parti d'un soutien technique d'experts.

L'application de ces concepts à la pratique professionnelle implique la communication des stratégies efficaces des ISSM à but non lucratif pour protéger leurs organisations contre les cybermenaces et les cyberattaques. Les résultats de ma recherche impliquent que l'application de stratégies de cybersécurité ISSM réussies peut fournir à d'autres ISSM à but non lucratif un guide essentiel sur l'évaluation et l'atténuation des vulnérabilités des cybermenaces. Les conclusions de mon étude s'alignent sur la TPS, car les ISSM réussis dans les organismes à but non lucratif combinent les trois stratégies principales pour réaliser des opérations efficaces, sécurisées et durables.

Implications pour le changement social

Les implications de cette recherche en matière de changement social incluent l'impact possible de stratégies de cybersécurité efficaces pour les ISSM des organisations à but non lucratif afin d'atténuer et de prévenir les attaques potentielles de cybersécurité. L'un des défis les plus importants auxquels sont confrontés les ISSM à but non lucratif est la capacité de déjouer les cyberattaques ciblant leurs organisations. Comme les conclusions de cette étude de recherche, la mise en œuvre de pratiques pratiques de cybersécurité pratiques illustre que les ISSM à but non lucratif ayant une meilleure compréhension des méthodologies de cybersécurité offrent des stratégies durables sur la cybersécurité pour atténuer les cyberattaques futures et stimuler leur perspective pour des opérations organisationnelles durables. La durabilité des organismes sans but lucratif garantit à la société des avantages ininterrompus, y compris la croissance économique grâce à des opportunités d'emploi, la promotion de l'engagement civique et la promotion des capacités de leadership.

Comme indiqué dans les conclusions de l'étude de recherche, les ISSM réussis dans les organisations à but non lucratif devraient appliquer plusieurs approches pour éviter les attaques de cybersécurité, y compris (a) la stratégie de cybersécurité, (b) la sensibilisation à la cybersécurité et (c) la dépendance aux services et à l'infrastructure des fournisseurs tiers. L'application de ces stratégies peut inspirer confiance aux consommateurs au point de créer une plus grande prospérité économique. Les implications positives du changement social comprennent l'autonomisation d'autres ISSM dans les organisations à but non lucratif, les établissements universitaires et les

nouveaux organismes à but non lucratif avec des stratégies et des ressources pratiques qui profitent à l'ensemble de la communauté. Les avantages pour la collectivité comprennent l'offre de possibilités d'emploi, la possibilité d'attirer l'attention du public sur les questions de société et la possibilité pour les collectivités de contourner des problèmes particuliers qui les touchent. En outre, les ISSM à but non lucratif peuvent changer leur point de vue sur les stratégies de cybersécurité, étendre leurs opérations et aider d'autres organisations à but non lucratif. Les ISSM survivent aux cyberattaques et aux attaques pour atteindre la croissance en employant des résidents au sein de la communauté et en stimulant le cycle de vie socio-économique général.

Recommandations d'action

Cette étude qualitative multicase visait à explorer les stratégies que les ISSM des organisations à but non lucratif utilisent pour se protéger contre les cyberattaques. En général, jusqu'à 3 % des organismes sans but lucratif signalent des cas de données volées ou perdues (Romanosky, 2016). Dans le passé, beaucoup considéraient les cyberattaques comme s'il s'agissait d'un problème qui ne touchait que les organisations à but lucratif. Cependant, l'augmentation des cas de cyberattaques parmi les organisations à but non lucratif continue d'affecter leur existence et leurs opérations (Carrapico et Farrand, 2017). À l'heure actuelle, cependant, les dirigeants des organismes sans but lucratif reconnaissent l'existence des cyberattaques et expriment des préoccupations en matière de cybersécurité, mais il existe un écart important entre l'inquiétude et la prise de mesures (Romanosky, 2016).

Cette étude de recherche s'est concentrée sur l'analyse de nombreuses sources de littérature savante, les réponses des participants aux ISSM à but non lucratif aux entrevues et les documents d'archives, qui offraient tous un soutien corroborant ainsi que la triangulation pendant le processus de collecte de données, pour répondre à la question de recherche de savoir quelles sont les stratégies que les ISSM dans les organisations à but non lucratif emploient pour se protéger contre les cyberattaques? Sur la base de l'analyse des données triangulées et des fréquences des réponses des nœuds codés, trois thèmes importants sont ressorties : a) stratégie de cybersécurité, b) sensibilisation à la cybersécurité et c) dépendance à l'égard des services et de l'infrastructure des fournisseurs tiers.

Sur la base de stratégies uniques et pratiques que les ISSM des organisations à but non lucratif utilisent pour éviter les cyberattaques, je recommande les actions suivantes aux dirigeants des organisations à but non lucratif, aux futurs ISSM dans les organisations à but non lucratif et aux nouvelles organisations à but non lucratif en général pour sécuriser leurs informations en utilisant les meilleures interventions de cybersécurité:

1. Évaluer la santé en matière de cybersécurité en évaluant l'environnement actuel des cybermenaces; classer le type de données de l'organisation à protéger; identifier les menaces, les vulnérabilités et les risques internes et externes; et en mettant l'accent sur les types de cybermenaces probables.

2. Élaborer et exécuter un plan stratégique complet sur la cybersécurité, y compris des politiques et des procédures visant à protéger les données sensibles et probablement sensibles.

Le plan stratégique sur la cybersécurité devrait établir au minimum ce qui suit :

a. Le mécanisme d'authentification à deux facteurs pour les utilisateurs valides (identifiant et mot de passe);

b. Ordinateurs de l'entreprise avec un logiciel antivirus installé, un logiciel malveillant et un logiciel anti-espion; et les correctifs fréquemment mis à jour du système d'exploitation de l'ordinateur;

c. Sécurisez les connexions réseau Wi-Fi et Internet à l'aide de méthodes de cryptage des données et de pare-feu.

d. Chiffrement de bout en bout des données et tokenisation pour garantir des transactions organisationnelles sécurisées ; et

e. Protection des sites Web de l'organisation à l'aide de fonctionnalités de transaction de données sécurisées telles que la conformité des données PCI, les pare-feu, SSL et les routeurs.

1. Évaluez les capacités informatiques internes et envisagez d'embaucher des fournisseurs tiers pour utiliser leurs compétences d'experts, réduire les responsabilités et les risques liés à l'infrastructure et atténuer les pertes éventuelles de violation de données en utilisant la garantie du fournisseur en matière de violation de données sur la cybersécurité.

2. Sensibiliser à la cybersécurité en formant les employés pour les doter de connaissances sur la protection des données, la protection des données organisationnelles et des consommateurs, et les règles d'engagement quotidiennes pour assurer la réussite des opérations organisationnelles.

Mon plan pour diffuser les conclusions et les recommandations de l'étude est de fournir des fiches d'information sommaires aux cinq ISSM qui ont participé à cette étude. Je vais leur expliquer de manière assez détaillée les résultats de la recherche et donner des détails spécifiques sur la façon dont les organisations à but non lucratif peuvent appliquer la même chose. Je partagerai également les résultats de la recherche et les recommandations avec les établissements universitaires de la localité, principalement par le biais de séminaires et d'ateliers organisés. En outre, en tant que conférencier invité, j'offrirai des services de consultants sur les stratégies réussies pour les ISSM dans des organisations à but non lucratif dans le cadre d'ateliers et de conférences parrainés par des organisations non gouvernementales ciblant les organisations à but non lucratif. De plus, je chercherai également à exploiter les publications de l'industrie et les revues universitaires pour diffuser les résultats de mes recherches.

Recommandations pour d'autres recherches

Les résultats, les conclusions et les recommandations de cette étude peuvent contribuer aux recherches existantes, ainsi qu'aux recherches futures sur les meilleures pratiques que les ISSM des organisations à but non lucratif utilisent pour protéger et défendre leurs organisations contre les cyberattaques. Le principal résultat de ces pratiques est la réalisation d'opérations organisationnelles réussies et durables. Étant

donné que cette étude ne couvrait que les organisations à but non lucratif du Maryland et du district de Columbia, ma recommandation est de faire mener d'autres études dans un autre emplacement géographique. Fonder une étude similaire sur un emplacement différent et des données régionales différentes permettrait des comparaisons avec ce que cette découverte de recherche a réalisé. De plus, étant donné que cette étude a mobilisé une population d'échantillons de cinq ISSM, je recommanderais aux chercheurs d'inclure une taille d'échantillon plus grande dans les études futures pour voir si les résultats changeraient ou resteraient similaires. En outre, je recommande que des études similaires fassent intervenir différentes populations autres que les ISSM et différentes méthodes de collecte de données autres que les entrevues à l'avenir. Les recommandations permettront d'obtenir une constatation plus élaborée, qui sera plus globale que les constatations actuelles de la présente étude.

Dans la section 1, les limites portaient sur la question de savoir si les participants comprendraient les questions d'entrevue dans la mesure où ils fourniraient des réponses honnêtes, s'ils seraient disponibles pendant les entrevues personnelles pour assurer la collecte de données en temps opportun, et si la réalisation d'entrevues semi-structurées et l'évaluation des documents archivistiques de l'entreprise fourniraient des données adéquates répondant à la question de recherche globale. Le facteur limitant spécifique influençant le processus de recherche a été de trouver des ISSM travaillant dans des organisations à but non lucratif dans le Maryland et DC et disposés à participer à l'étude. Cette découverte a pris du temps et m'a finalement permis de prendre plus de temps pour trouver des participants viables à la recherche. Néanmoins, une fois que les ISSM ont

accepté de participer, aucune autre question importante n'a été soulevées. Les données d'archives disponibles et les entrevues ont donné lieu à des réponses honnêtes de la part des participants, fournissant ainsi suffisamment de données pour les analyses. À l'avenir, je recommande que les chercheurs aient beaucoup plus de temps pour permettre la recherche de participants viables à la recherche.

Réflexions

Travailler à la réalisation de cette étude doctorale DIT m'a offert une expérience de croissance remarquable. Ce processus a été fructueux et mouvementé à la fois parce que j'ai rencontré de nombreuses situations prolifiques qui étaient au-delà de mon imagination. J'ai acquis plus de connaissances concernant les stratégies de cybersécurité efficaces dans les organisations à but non lucratif, qui se sont avérées efficaces pour contrecarrer les menaces de cybersécurité. Plus précisément, j'ai appris les pratiques stratégiques que les ISSM des organisations à but non lucratif du Maryland et de DC utilisent pour relever les défis de la cybersécurité. Je suis optimiste quant au partage et à l'application de mes résultats de recherche avec des établissements universitaires, des organisations à but non lucratif, des établissements universitaires et des entités gouvernementales. Les résultats de l'étude de recherche peuvent ajouter beaucoup plus de contenu à la recherche existante et future, en particulier en équipant les ISSM pour protéger et protéger leurs organisations à but non lucratif contre les cyberattaques. Ces ISSM qualifiés enregistreraient à leur tour des opérations organisationnelles efficaces, durables et sûres.

Après la réalisation de recherches littéraires, un préjugé personnel a formé une notion préconçue que la plupart des ISSM n'étaient pas au courant et n'ont pas mis en œuvre suffisamment d'interventions en matière de cybersécurité pour remédier aux vulnérabilités potentielles des cybermenaces. De plus, mon expérience et mon expertise dans le domaine informatique travaillant pour différentes organisations avec des plans de cybersécurité élaborés ont alimenté cette idée. Tous les participants ont servi avec succès en tant qu'ISSM dans des organisations à but non lucratif et ont compris très clairement les vulnérabilités des cybermenaces, y compris les conséquences potentielles affectant leurs opérations organisationnelles. En menant les entrevues semi-structurées, je me suis assuré de ne pas diriger ou diriger les participants, notamment en évitant les réactions négatives ou positives à l'égard de leurs réponses. Je crois que les répondants ont fourni des réponses honnêtes et franches aux douze questions de l'entrevue. Je suis également convaincu que mes actions n'influencent jamais, à un moment donné, négativement les réponses des participants.

À la fin de mon étude de recherche, la notion préconçue que j'avais changée à propos des ISSM réussis dans les organisations à but non lucratif utilise des stratégies de cybersécurité efficaces. L'analyse documentaire a présenté des résultats indiquant que le recours à des fournisseurs tiers était risqué et coûteux. Cependant, après avoir analysé les entrevues avec les participants et les données des documents d'archives, ma pensée a changé. Les ISSM efficaces dans les organisations à but non lucratif ont évalué leurs risques et ont généralement déterminé que les fournisseurs tiers étaient adaptables et évolutifs, fiables dans leur expertise et rentables. En outre, des ISSM efficaces ont établi

le fait que les fournisseurs tiers limitaient leurs responsabilités chaque fois que des violations de données se produisaient. Bien que l'objectif de cette étude de recherche n'ait impliqué qu'une petite population dans le Maryland et DC, les résultats de l'étude capturent très probablement le tableau général des ISSM dans les organisations à but non lucratif dans d'autres zones géographiques et mettent en œuvre des actions stratégiques contre les menaces de cybersécurité.

Conclusion

Cette étude de cas qualitative multiple visait à explorer les stratégies que les ISSM des organisations à but non lucratif utilisent pour se protéger contre les cyberattaques. Les résultats de l'étude de recherche révèlent des stratégies efficaces que les ISSM des organisations à but non lucratif utilisent pour protéger leurs organisations contre les cyberattaques. Trois thèmes principaux se sont concrétisés en ce qui concerne les résultats de la recherche, corroborant l'analyse documentaire, le cadre conceptuel de la TPS et l'ensemble des connaissances existantes. Les résultats de l'étude de recherche indiquent ce qui suit sur les ISSM dans les organisations à but non lucratif; a) mettre en œuvre une stratégie de cybersécurité axée sur la protection, la défense et la réaction aux cyberattaques; (b) sont conscients des menaces de cybersécurité, et (c) dépendent de fournisseurs tiers pour l'infrastructure de services et la défense de la cybersécurité. Les ISSM des organisations à but non lucratif qui déjouent avec succès les cyberattaques peuvent contribuer énormément à la croissance économique parce qu'ils emploient des résidents au sein de la communauté, ce qui finit par stimuler le cycle de vie socio-économique.

En outre, les ISSM des organisations à but non lucratif qui mettent en œuvre des stratégies efficaces peuvent inspirer confiance aux consommateurs, ce qui, à son tour, déclencherait une prospérité économique significative. En réalité, la menace mondiale de cybersécurité ne cesse d'évoluer au fil du temps, ce qui confère aux ISSM une plus grande responsabilité dans l'évaluation des vulnérabilités et dans le développement et l'exécution des meilleures stratégies de cybersécurité. À son tour, il garantit des opérations sécurisées et durables pour les organisations à but non lucratif.

References

Alhassan, I., Sammon, D., et Daly, M. (2016). Activités de gouvernance des données : analyse de la documentation. *Journal of Decision Systems, 25*(sup1), 64-75. https://doi.org/10.1080/12460125.2016.1187397

Alkalbani, A., Deng, H., Kam, B., &Zhang, X. (2017). Information security compliance in organizations: An institutionalperspective. *Gestion des données et de l'information, 1(2),* 104-114. https://doi.org/10.1515/dim-2017-0006

Almubark, A., Hatanaka, N., Uchida, O., et Ikeda, Y. (2016). Identifier les mécanismes des incidents de sécurité de l'information au moyen de variables de culture organisationnelle et d'échantillonnage. *International Journal of Cyber-Security and Digital Forensics, 5*(2), 61-74. https://doi.org/10.17781/p002025

Alshahrani, M., &Traore, I. (2019). Authentification mutuelle sécurisée et contrôle d'accès automatisé pour la maison intelligente IoT à l'aide de la chaîne de hachage à clé cumulative. *Journal of Information Security and Applications, 45,*156-175. https://doi.org/10.1016/j.jisa.2019.02.003

Al-Taie, M., Lane, M., &Cater-Steel, A. (2018). Une évaluation empirique de l'instrument d'attentes en matière de rôles du DPI à l'aide de la modélisation des trajectoires pls. *Communications of the Association for Information Systems, 42,* 1-20. https://doi.org/10.17705/1cais.04201

Anand, R., Medhavi, S., Soni, V., Malhotra, C., &Banwet, D. K. (2018). Transformer la gouvernance de la sécurité de l'information en Inde (une étude de cas basée sur SAP-LAP de la sécurité, de la politique informatique et de la gouvernance

électronique). *Information and Computer Security*, *26*(1), 58-90. https://doi.org/10.1108/ics-12-2016-0090

Aranda, M., Hurtado, M.D. &Topa, G. (2018). Rupture de contrat psychologique et comportements de citoyenneté organisationnelle dans le bénévolat: Le rôle de médiateur de l'affect et la modération de l'âge des bénévoles. *Voluntas, 29***,** 59-70. https://doi.org/10.1007/s11266-017-9923-4

Assarroudi, A., Nabavi, F. H., Armat, M. R., Ebadi, A., &Vaismoradi, M. (2018). Analyse qualitative dirigée du contenu: La description et l'élaboration de ses méthodes sous-jacentes et le processus d'analyse des données. *Journal of Research in Nursing*, *23*(1), 1-14. https://doi.org/10.1177/174498711774166

Atoum, I., &Otoom, A. (2016). Modèle de rendement holistique pour les cadres de mise en œuvre de la cybersécurité. *International Journal of Security and Its Applications, 10*(3), 111-120. https://doi.org/10.14257/ijsia.2016.10.3.10

Attaran, M. (2017). Technologie de cloud computing : Tirer parti de la puissance d'Internet pour améliorer les performances de l'entreprise. *Journal of International Technology and Information Management, 26*(1), 112-137. https://doi.org/10.1016/j.ijinfomgt.2012.04.001.3

Azungah, T. (2018). Recherche qualitative : Approches déductives et inductives de l'analyse des données. *Qualitative Research Journal, 18*(4), 383-400. https://doi.org/10.1108/qrj-d-18-00035

Bach-Mortensen, A.M., &Montgomery, P. (2018). Quels sont les obstacles et les facilitateurs qui empêchent les organisations du secteur tiers (organismes à but

non lucratif) d'évaluer leurs services? Un examen systématique. *Revues systématiques*, *7*(1). 1-15. https://doi.org/10.1186/s13643-018-0681-1

Ballaro, J.M., &Polk, L. (2017). Développer une organisation pour la croissance future en utilisant la planification de la relève. *Organization Development Journal*, *35*(4), 41-42. https://www.isodc.org/page-1730212

Bamkin, M., Maynard, S., &Goulding, A. (2016). Théorie fondée et ethnographie combinées. *Journal of Documentation, 72*(2), 214-231. https://doi.org/10.1108/JD-01-2015-0007

Barlette, Y., Gundolf, K., &Jaouen, A. (2017). Comportement des PDG en matière de sécurité de l'information dans les PME : la propriété est-elle importante ? *Systèmes d'Information Et Management, 22*(3), 7-45,117. https://doi.org/10.3917/sim.173.0007

Baseri, Y., Hafid, A., &Cherkaoui, S. (2018). Confidentialité préservant un contrôle d'accès basé sur la localisation précis pour le cloud mobile. *Ordinateurs et sécurité, 73,*249-265. https://doi.org/10.1016/j.cose.2017.10.014

Baskerville, R. (2010). Conflits au troisième degré: guerrede l'information. *European Journal of Information Systems, 19*(1,) 1-4. https://doi.org/10.1057/ejis.2010.2

Bauer, S., Bernroider, E. W., &Chudzikowski, K. (2017). Mieux vaut prévenir que guérir ! Concevoir des programmes de sensibilisation à la sécurité de l'information pour surmonter le non-respect par les utilisateurs des politiques de sécurité de l'information dans les banques. *Computers &Security, 68*, 145-159. https://doi.org/10.1016/j.cose.2017.04.009

Benoot, C., Hannes, K., et Bilsen, J. (2016). The use of purposeful sampling in a qualitative evidence synthesis: A worked example on sexual adjustment to a cancer trajectory. *BMC Medical Research Methodology*, *16*(1), 1-12. https://doi.org/10.1186/s12874-016-0114-6

Bertoglio, D., &Zorzo, A. F. (2017). Vue d'ensemble et questions en suspens sur le test de pénétration. *Journal of the Brazilian Computer Society*, *23*(1), 1 https://doi.org/10.1186/s13173-017-0051-1

Bharathi, S. V. (2017). Prioriser et classer le spectre des risques liés à la sécurité des données volumineuses. *Global Journal of Flexible Systems Management*, *18*(3), 183-201. https://doi.org/10.1007/s40171-017-0157-5

Bidgoli, H. (2018). Déploiement de l'informatique en nuage : Qu'avons-nous appris des implémentations et des pratiques de la vie réelle? *Journal of Strategic Innovation and Sustainability*, *13*(1), 36-52. https://doi.org/10.33423/jsis.v13i1.594

Bildosola, I., Río-Belver, R., Cilleruelo, E., &Garechana, G. (2015). Conception et mise en œuvre d'un outil de décision d'adoption du cloud computing : Génération d'une route cloud. *PLOS ONE*, *10*(7), e0134563. https://doi.org/10.1371/journal.pone.0134563

Boddy, C. R. (2016). Taille de l'échantillon pour la recherche qualitative. *Qualitative Market Research*, *19*(4), 426-432. https://doi.org/10.1108/QMR-06-2016-0053

Boell, S. K. et Cecez-Kecmanovic, D. (2015). Debating systematic literature reviews (SLR) and their ramifications for IS: A rejoinder to Mike Chiasson, Briony Oates,

Ulrike Schultze, and Richard Watson. *Journal of Information Technology*, *30*(2), 188-193. https://doi.org/10.1057/jit.2015.15

Bordoff, S., Chen, Q. et Yan, Z. (2017). Cyberattaques, facteurs contributifs et stratégies de lutte : État actuel de la science de la cybersécurité. *Journal International Journal of Cyber Behavior, Psychology and Learning archive, 7*(4), 68-82. https://doi.org/10.4018/ijcbpl.2017100106

Bradshaw, C., Atkinson, S., et Doody, O. (2017). Utilisation d'une approche de description qualitative dans la recherche en soins de santé. *Recherche qualitative mondiale en soins infirmiers, 4*, 233339361774228. https://doi.org/10.1177/2333393617742282

Bridgen, S. (2017). Utilisation de la théorie des systèmes pour comprendre l'identité des conseils académiques : étude de cas. *NACADA Journal*, *37*(2), 9-20. https://doi.org/10.12930/NACADA-15-038

Brown, A., et Danaher, P. A. (2017). Principes du CHE : Faciliter des entretiens semi-structurés authentiques et dialogiques dans la recherche en éducation. *International Journal of Research &Method in Education, 42*(1), 76-90. https://doi.org/10.1080/1743727x.2017.1379987

Burns, A. J., Posey, C., Courtney, J. F., Roberts, T. L., et Nanayakkara, P. (2015). Sécurité des informations de l'organisation en tant que système adaptatif complexe : insights à partir de trois modèles basés sur des agents. *Frontières des systèmes d'information*, *19*(3), 509-524. https://doi.org/10.1007/s10796-015-9608-8

Cameron, R., Sankaran, S., &Scales, J. (2015). Utilisation de méthodes mixtes dans la recherche en gestion de projet. *Project Management Journal*, *46*(2), 90-104. https://doi.org/10.1002/pmj.21484

Carrapico, H., et Farrand, B. (2016). « Dialogue, partenariat et autonomisation pour la sécurité des réseaux et de l'information »: l'évolution du rôle du secteur privé, qui est passée d'objets de réglementation à des façonneurs de réglementation. *Crime, Law and Social Change*, *67*(3), 245-263. https://doi.org/10.1007/s10611-016-9652-4

Cataldi, S. (2018). Une proposition pour l'analyse de la dimension relationnelle dans les techniques d'entrevue: Une étude pilote sur les entrevues approfondies et les groupes de discussion. *Quality and Quantity*, *52*(1), 295-312. https://doi.org/10.1007/s11135-017-0468-9

Catota, F. E., Morgan, M. G., et Sicker, D.C. (2018). Capacités de réponse aux incidents de cybersécurité dans le secteur financier équatorien. *Journal of Cybersecurity, 4*(1), 1-20. https://doi.org/10.1093/cybsec/tyy002

Cavalcanti, M. F. R. (2017). Guidelines for qualitative research in organization studies: controversy and possibilities. *Administração: Ensino e Pesquisa, 18*(3), 457-488. https://doi.org/10.13058/raep.2017.v18n3.522

Caws, P. (2015). S ystems theory: Son past et potential. *Systems Research and Behavioral Science, 32*(5), 514-521. https://doi.org/10.1002/sres.2353

Cerniglia, J. A., Fabozzi, F. J., &Kolm, P. N. (2016). Meilleures pratiques en recherche pour les stratégies d'équité quantitatives. *Journal of Portfolio Management, 42*(5), 135-143. https://doi.org/10.3905/jpm.2016.42.5.135

Che-Hung, L., Jen, S. W., &Ching-Wei, L. (2017). Les concepts de big data appliqués dans la gestion des connaissances personnelles. *Journal of Knowledge Management, 21*(1), 213-230. https://doi.org/10.1108/JKM-07-2015-0298

Chen, D., Doumeingts, G., &Ducq, Y. (2012). A contribution of system theory to sustainable enterprise interoperability science base. *Ordinateurs dans l'industrie, 63*,844-857. https://doi.org/10.1016/j.compind.2012.08.005

Citera, E. (2017). La complexité de Keynes et de l'Institut de Santa Fe : mêmes concepts, méthodes différentes ? *Annales de la Fondazione Luigi Einaudi, 1,* 207-222. https://doi.org/10.26331/1010

Clubb, A.C., &Hinkle, J.C. (2015). La théorie de la motivation de la protection en tant que cadre théorique pour comprendre l'utilisation des mesures de protection. *Criminal Justice Studies, 28*(3), 336-355. https://doi.org/10.1080/1478601x.2015.1050590

Cobb, C., Sudar, S., Reiter, N., Anderson, R., Roesner, F., &Kohno, T. (2018). Sécurité informatique pour les technologies de collecte de données. *Development Engineering, 3,* 1-11. https://doi.org/10.1016/j.deveng.2017.12.002

Coetzee, C., Dewald, V. N., &Raju, E. (2016). Résilience aux catastrophes et théorie des systèmes adaptatifs complexes. *Disaster Prevention and Management, 25*(2), 196-211. https://doi.org/10.1108/dpm-07-2015-0153

Colorafi, K. J. et Evans, B. (2016). Méthodes descriptives qualitatives dans la recherche en sciences de la santé. *Health Environments Research &Design Journal, 9*(4), 16-25. https://doi.org/10.1177/1937586715614171

Conrad, L. Y., &Tucker, V.M. (2019). Rendre les choses tangibles : Tri des cartes hybrides dans le cadre d'entretiens qualitatifs. *Journal of Documentation, 75*(2), 397-416. https://doi.org/10.1108/jd-06-2018-0091

Constantinou, C. S., Georgiou, M., &Perdikogianni, M. (2017). Une méthode comparative pour la saturation des thèmes (CoMeTS) dans les entretiens qualitatifs. *Qualitative Research,* 17(5), 571-588. https://doi.org/10.1177/1468794116686650

Corti, L., &Fielding, N. (2016). Opportunities from the digital revolution: Implications for researching, publishing, and consuming qualitative research. *Sage Open, 6*(4), 1-13. https://doi.org/10.1177/2158244016678912

Daher, M., Carré, D., Jaramillo, A., Olivares, H., &Tomicic, A. (2017). Expérience et signification de la recherche qualitative : un examen conceptuel et une proposition de dispositif méthodologique. *Forum : Recherche sociale qualitative, 18*(3), 1-24. https://doi.org/10.17169/fqs-18.3.2696

Daniel Ani, U. P., He, H.M., &Tiwari, A. (2016). Approche d'évaluation des capacités humaines pour la cybersécurité dans les infrastructures industrielles essentielles. In D. Nicholson (Ed.), *Advances in human factors in cybersecurity. Advances in Intelligent systems and computing* (Vol. 501, pp. 169-182). Springer. https://doi.org/10.1007/978-3-319-41932-9_14

Daniel, B. K. (2018). Vérification empirique du cadre « TACT » pour l'enseignement de la rigueur dans la méthodologie de recherche qualitative. *Qualitative Research Journal, 18*(3), 262-275. https://doi.org/10.1108/qrj-d-17-00012

Das, R., Jain, K. K., &Mishra, S. K. (2018). Recherche archivistique : une méthode négligée dans les études d'organisation. *Benchmarking, 25*(1), 138-155. https://doi.org/10.1108/bij-08-2016-0123

Dasgupta, M. (2015). Explorer la pertinence de la recherche d'études de cas. *Vision, 19*(2), 147-160. https://doi.org/10.1177/0972262915575661

Davidson, E., Edwards, R., Jamieson, L., et Weller, S. (2019). Big data, style qualitatif : méthode d'étendue et de profondeur pour travailler avec de grandes quantités de données qualitatives secondaires. *Quality and Quantity*, *53*(1), 363-376. https://doi.org/10.1007/s11135-018-0757-y

De Boer, L., &Andersen, P. H. (2016). Apprendre d'une conversation intelligente. *IMP Journal, 10*(3), 512-539. https://doi.org/10.1108/imp-12-2015-0070

DeGama, N., Elias, S., &Peticca-Harris, A. (2019). Le bon universitaire : Réinventer une bonne recherche dans les études d'organisation et de gestion. *Qualitative Research in Organizations and Management: An International Journal, 14*(1), 2-9. https://doi.org/10.1108/qrom-03-2019-681

DiMase, D., Collier, Z. A., Heffner, K., &Linkov, I. (2015). Cadre d'ingénierie des systèmes pour la cybersécurité physique et la résilience. Environment Systems and Decisions, 35(2), 291-300. https://doi.org/10.1007/s10669-015-9540-y

. *Environment Systems and Decisions*, *35*(2), 291-300. https://doi.org/10.1007/s10669-015-9540-y

Doherty, N. F. et Tajuddin, S. T. (2018). Vers une théorie centrée sur l'utilisateur de la conformité à la sécurité des informations axée sur la valeur. *Information Technology &People*, *31*(2), 348-367. https://doi.org/10.1177/1715163517701470

Poupée, J. L. (2017). Entrevues structurées : Développer les compétences en entrevue dans les cours de gestion des ressources humaines. *Management Teaching Review*, *3*(1), 46-61. https://doi.org/10.1177/2379298117722520

Dove, E. S. (2018). The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era. *The Journal of Law, Medicine &Ethics*, *46*(4), 1013-1030. https://doi.org/10.1177/1073110518822003

Drack, M., &Pouvreau, D. (2015). Sur l'histoire de la « Systemologie générale » de Ludwig von Bertalanffy, et sur sa relation avec la cybernétique - partie III: convergences et divergences. *International journal of general systems*, *44*(5), 523-571. https://doi.org/10.1080/03081079.2014.1000642

Efthymiopoulos, M. P. (2019). Un cadre de cybersécurité pour le développement, la défense et l'innovation à l'OTAN. *Journal of Innovation and Entrepreneurship*, *8*(1). 1-26. https://doi.org/10.1186/s13731-019-0105-z

El-Bendary, M. (2017). FEC a fusionné avec l'approche de double sécurité basée sur la stéganographie d'image cryptée dans un but différent en présence de bruit et de différentes attaques. *Multimedia Tools and Applications*, *76*(24), 26463-26501. https://doi.org/10.1007/s11042-016-4177-5

Elman, C., Gerring, J., et Mahoney, J. (2016). Étude de cas. *Sociological Methods &Research, 45,* 375-391. https://doi.org/10.1177/0049124116644273

Eriksson, P. E. (2017). Stratégies d'approvisionnement pour améliorer l'exploration et l'exploitation dans les projets de construction. *Journal of Financial Management of Property and Construction, 22*(2), 211-230. https://doi.org/10.1108/jfmpc-05-2016-0018

Erlingsson, C., &Brysiewicz, P. (2017). Un guide pratique pour faire de l'analyse de contenu. *African Journal of Emergency Medicine, 7*(3), 93-99. https://doi.org/10.1016/j.afjem.2017.08.001

Fal', O.M. (2017). Normalisation de la sécurité des technologies de l'information. *Cybernetics and Systems Analysis, 53*(1), 78-82. https://doi.org/10.1007/s10559-017-9908-8

Farooq, M.B., &de Villiers, C. (2017). Entretiens de recherche qualitative téléphonique : Quand les considérer et comment les faire. *Meditari Accountancy Research, 25*(2), 291-316. https://doi.org/10.1108/MEDAR-10-2016-0083

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., &Smeraldi, F. (2016). Approches d'aide à la décision pour l'investissement dans la cybersécurité. *Decision Support Systems, 86,*13-23. https://doi.org/10.1016/j.dss.2016.02.012

Fletcher, A. J. (2017). Application du réalisme critique à la recherche qualitative : la méthodologie rencontre la méthode. *International Journal of Social Research Methodology: Theory &Practice, 20,* 181-194. https://doi.org/10.1080/13645579.2016.1144401

Fusch, P., Fusch, G. E., et Ness, L. R. (2018). Denzin's Paradigm Shift: Revisiting Triangulation in Qualitative Research. *Journal of Social Change, 10*(1), 19-32. https://doi.org/10.5590/JOSC.2018.10.1.02

Gammelgaard, B. (2017). Éditorial : L'étude de cas qualitative. *International Journal of Logistics Management, 28*(4), 910-913. https://doi.org/10.1108/IJLM-09-2017-0231

Garlinec, D., Možnik, D., &Guberina, B. (2017). Cybersécurité et cyberdéfense: approche stratégique au niveau national. *Journal for Control, Measurement, Electronics, Computing and Communications, 58*(3), 273-286. https://doi.org/10.1080/00051144.2017.1407022

Gaus, N. (2017). Selecting research approaches and research designs: A reflective essay. *Qualitative Research Journal, 17*(2), 99-112. https://doi.org/10.1108/QRJ-07-2016-0041

Gordon, L. A., Loeb, M. P., Lucyshyn, W., &Zhou, L. (2015). Accroître les investissements en cybersécurité dans les entreprises du secteur privé. *Journal of Cybersecurity, 1*(1), 3-17 https://doi.org/10.1093/cybsec/tyv011

Greenwood, M. (2016). Approuver ou améliorer l'éthique de la recherche dans les revues de gestion. *Journal of Business Ethics, 137*(3), 507-520. https://doi.org/10.1007/s10551-015-2564-x

Grimaldo, F., Marušić, A., &Squazzoni, F. (2018). Fragments d'examen par les pairs : Analyse quantitative de la littérature (1969-2015). *PLoSONE, 13*(2), e0193148. https://doi.org/10.1371/journal.pone.0193148

Hammarberg, K., Kirkman, M., &de Lacey, S. (2016). Méthodes de recherche qualitative: quand les utiliser et comment les juger. *Human Reproduction, 31*(3), 498-501. https://doi.org/10.1093/humrep/dev334

Hampton, J. O., MacKenzie, D. I., et Forsyth, D.M. (2019). Combien en échantillonner? Lignes directrices statistiques pour le suivi des résultats en matière de bien-être animal. *PLOS ONE, 14*(1), e0211417. https://doi.org/10.1371/journal.pone.0211417

He, W., &Zhang, Z. (2019). Programmes de formation et de sensibilisation à la cybersécurité d'entreprise : Recommandations pour réussir. *Journal of Organizational Computing and Electronic Commerce, 29*(4), 249-257. https://doi.org/10.1080/10919392.2019.1611528

Heesen, R., Bright, L. K., &Zucker, A. (2016). Justification de la triangulation méthodologique. *Synthese, 196*(8), 3067-3081. https://doi.org/10.1007/s11229-016-1294-7

Hennink, M.M., Kaiser, B. N., &Marconi, V.C. (2017). Saturation du code ou saturation du sens : Combien d'entrevues suffisent? *Qualitative Health Research, 27,* 591-608. https://doi.org/10.1177/1049732316665344

Henry, C., &Foss, L. (2015). Sensible à la casse? Un examen de la littérature sur l'utilisation de la méthode cas dans la recherche d'entrepreneuriat. *International Journal of Entrepreneurial Behaviour &Research, 21*(3), 389-409. https://doi.org/10.1108/IJEBR-03-2014-0054

Hodiamont, F., Jünger, S., Leidl, R., Bernd, O.M., Schildmann, E., &Bausewein, C. (2019). Comprendre la complexité – la situation des soins palliatifs en tant que système adaptatif complexe. *BMC Health Services Research, 19.* https://doi.org/10.1186/s12913-019-3961-0

Hof, B. E. (2018). Le cybernetic "general model theory »: Unifying science or epistemic change? *Perspectives on Science, 26*(1), 76. http://search.ebscohost.com/login.aspx?direct=true&db=edb&AN=127769651&site=eds-live

Holland, A. (2017). Stratégies des dirigeants d'organismes sans but lucratif pour capter l'attention de grands donateurs engagés (thèse de doctorat). ProQuest Digital Dissertations &Theses Base de données mondiale. (UMI n° 10253906)

Holtfreter, R. E. et Harrington, A. (2015). Tendances en matière de violation de données aux États-Unis. *Journal of Financial Crime, 22*(2), 242-260. https://doi.org/10.1108/JFC-09-2013-0055

Horne, C. A., Ahmad, A., &Maynard, B. S. (2016,décembre). *Une théorie sur la sécurité de* l'information [Présentation de l'article]. The 27th Australasian Conference on Information Systems, Wollongong, Australia. https://www.researchgate.net/publication/318589055_A_Theory_on_Information_Security

Horvath, M., &Lovasz, A. (2018). Programmation dela circle v icious: Austen, Deleuze et viral repetition. *Rhizomes: Cultural Studies in Emerging Knowledge,* (33), 15. http://www.rhizomes.net/issue33/pdf/horvath.pdf

Hubbard, T., Fabius, J. A., &Steinhoff, J.C. (2019). Exploiter et protéger les actifs de données dans une entreprise financière du 21e siècle. *Journal of Government Financial Management, 67*(4), 34-41. https://institutes.kpmg.us/content/dam/institutes/en/government/pdfs/2019/aga-winter-cyber.pdf

Humphreys, M. (2015). Réflexions sur l'éthique de l'expérimentation sociale. *Journal of Globalization and Development, 6*(1), 87-112. https://doi.org/10.1515/jgd-2014-0016

La F ederation internationale des sociétés de Red Cross et duCroissant-Rouge. (2019). Bénévolat policy. Consulté le 26 février 2019sur https://media.ifrc.org/ifrc/what-we-do/volunteers/volunteering-policy/

Iivari, N. (2018). Utilisation de la vérification des membres dans la pratique de recherche interprétative. *Information Technology &People, 31*(1), 111-133. https://doi.org/10.1108/ITP-07-2016-0168

Jagalur, P. K., Levin, P. L., Brittain, K., Dubinsky, M., Landau-Jagalur, K., &Lathrop, C. (2018, novembre). *Cybersécurité pour lacivil society*. En 2018 IEEE International Symposium on Technology and Society (ISTAS; pp. 102-107). IEEE.

Jalali, M. S. et Kaiser, J. P. (2018). Cybersecurity in Hospitals: A Systematic, Organizational Perspective. *Journal of Medical Internet Research, 20*(5), 1-16. https://doi.org/10.2196/10059

Junior, N. D. S. F. D. (2016). Modèle dynamique de coût de la qualité basé sur la théorie de la complexité. *International Journal of Quality &Reliability Management, 33*(5), 633-653. https://doi.org/10.1108/ijqrm-07-2014-0085

Kajiyama, T., Jennex, M., &Addo, T. (2017). Cloud ou non dans le cloud : comment les risques et les menaces affectent les décisions d'adoption du cloud. *Information and Computer Security, 25*(5), 634-659. https://doi.org/doi.org/10.1108/ICS-07-2016-0051

Kallio, H., Pietilä, A., Johnson, M., &Kangasniemi, M. (2016). Revue méthodologique systématique : Élaboration d'un cadre pour un guide d'entrevue semi-structuré qualitatif. *Journal of Advanced Nursing, 72,* 2954-2965. https://doi.org/10.1111/jan.13031

Kayaalp, M. (2018). La vie privée des patients à l'ère des mégadonnées. *Balkan Medical Journal, 35*(1), 8-17. https://doi.org/10.4274/balkanmedj.2017.0966

Kholidy, H. A., Erradi, A., Abdelwahed, S., &Baiardi, F. (2016). Une approche d'atténuation des risques pour un système autonome de réponse aux intrusions dans le cloud. *Computing, 98*(11), 1111-1135. https://doi.org/10.1007/s00607-016-0495-8

Kim, S. S. et Kim, Y. J. (2017). L'effet des connaissances en matière de conformité et des systèmes de prise en charge de la conformité sur le comportement de conformité en matière de sécurité des informations. *Journal of Knowledge Management, 21*(4), 986-1010. https://doi.org/10.1108/jkm-08-2016-0353

Kordova, S. K., Frank, M., et Miller, A. S. (2018). Systèmes d'education—Voir le forest à travers les trees. *Systèmes,* 6(3), 29. https://doi.org/10.3390/systems6030029

Korrapati, R. (2016). *Five chapter model for research thesis writing: 108 practicallLessons.* Diamond Pocket Books.

Krippner, S., Ruttenber, A. J., Engelman, S. R., &Granger, D. L. (1985). Towards the application of general systems theory in humanistic psychology. *Systems Research, 2*(2), 105-115. https://doi.org/10.1002/sres.3850020203

Kristof, V. A., Verschraegen, G., Valentinov, V., &Gruezmacher, M. (2019). Le social, l'écologique et l'adaptatif. Vsur la théorie générale des systèmes de Bertalanffy et la gouvernance adaptative des systèmes socio-écologiques. *Systems Research and Behavioral Science, 36*(3), 308-321. https://doi.org/10.1002/sres.2587

Kude, T., Hoehle, H., &Sykes, T. A. (2017). Violations de données volumineuses et stratégies de rémunération des clients. *International Journal of Operations &Production Management, 37*(1), 56-74. https://doi.org/10.1108/IJOPM-03-2015-0156

Kuerbis, B., &Badiei, F. (2017). Mapping the cybersecurity institutional landscape », *Digital Policy, Regulation and Governance, 19*(6), 466-492. https://doi.org/10.1108/DPRG-05-2017-0024

Lanz, J. (2017). Le dirigeant principal de la sécurité de l'information : Le nouveau directeur financier de la sécurité de l'information. *CPA Journal, 87*(6), 52. https://www.cpajournal.com/2017/06/23/chief-information-security-officer/

Larkin, M., Shaw, R., &Flowers, P. (2019). Conceptions et procédés multispectivals dans la recherche interprétative en analyse phénoménologique. *Qualitative Research in Psychology*, *16*(2), 182-198. https://doi.org/10.1080/14780887.2018.1540655

Lee, C. I. S. G. (11 mars 2016). Big Data in Management Research (No. EPS-2016-365-ORG). ERIM Ph.D. Series Research in Management. Université Erasmus de Rotterdam. http://hdl.handle.net/1765/79818

Leung, L. (2015). Validité, fiabilité et généralisabilité de la recherche qualitative. *Journal of family medicine and primary care*, *4*(3), 324. https://doi.org/10.4103/2249-4863.161306

Levesque, R., Walsh, D., et Whyte, D. (2015). Sécuriser le cyberespace : Vers un programme de recherche et de pratique. *Technology Innovation Management Review*, *5*(11), 26-34. https://search.proquest.com/docview/1736797748?accountid=45049

Libicki, M. (2017a). La convergence de l'information warfare. *Strategic Studies Quarterly*, *11*(1), 49-65. http://www.jstor.org/stable/26271590

Libicki, M.C. (2017b). Deuxième acte dans le cyberespace. *Journal of Cybersecurity*, *3*(1), 29-35. https://doi.org/10.1093/cybsec/tyw014

Lim, C., Kim, M., Kim, K., Kim, K., &Maglio, P. P. (2018). Utilisation des données pour faire progresser le service : Questions de gestion et implications théoriques de la recherche-action. *Journal of Service Theory and Practice*, *28*(1), 99-128. https://doi.org/10.1108/JSTP-08-2016-0141

Liu, Y.-T., Du, D., Xia, Y.-B., Cpoule, H.-B., Zang, B.-Y &Liang, Z. (2018). SplitPass: Un gestionnaire de mots de passe biparte qui se méfie mutuellement. *Journal of Computer Science and Technology, 33*(1), 98-115. https://doi.org/10.1007/s11390-018-1810-y

Lucas, S. R. (2016). Où le caoutchouc rencontre la route: Probabilité et non probabilite moments dans l'expérience, interview, archivage, administration, et la collecte de données ethnographiques. *Socius, 2 ans,* 2378023116634709.

MacDougall, R. (2019). Physique sympathique: Le moteur keely et les lois de la thermodynamique dans la culture du XIXe siècle. *Technology and Culture, 60*(2), 438-466. https://doi.org/10.1353/tech.2019.0031

Madill, A. et Sullivan, P. (2018). Miroirs, portraits et vérification des membres : Gérer les moments difficiles d'échange de connaissances en sciences sociales. *Qualitative Psychology, 5*(3), 321-339. https://doi.org/10.1037/qup0000089

Majid, M. A., Othman, M., Mohamad, S. F., Lim, S. A., &Yusof, A. (2017). Piloting for interviews in qualitative research: Operationalization and lessons learned. *International Journal of Academic Research in Business and Social Sciences, 7*(4). https://doi.org/10.6007/ijarbss/v7-i4/2916

Malgieri, G., &Comandé, G. (2017). Pourquoi un droit à la lisibilité de la prise de décision automatisée existe-t-il dans le règlement général sur la protection des données? *International Data Privacy Law, 7*(4), 243-265. https://doi.org/10.1093/idpl/ipx019

Maras, M.-H. (2015). Internet des objets : répercussions sur la sécurité et la protection de la vie privée. *International Data Privacy Law, 5*(2), 99-104. https://doi.org/10.1093/idpl/ipv004

Marchisotti, G. G., Joia, L. A., &De Carvalho, R.B. (2019). La représentation sociale du cloud computing selon les professionnels brésiliens des technologies de l'information. *Revista De Administração De Empresas, 59*(1), 16-28. https://doi.org/10.1590/S0034-759020190103

Margaret, M.M. (2016). Étude de cas : Quoi, pourquoi et comment? *South Asian Journal of Management, 23*(3), 218-221. https://search.proquest.com/docview/1845776117?accountid=45049

Marshall, C. et Rossman, G.B. (2016). Designing qualitative research (6e édition). Sauge.

Martin, K. et Murphy, P. (2017). Le rôle de la confidentialité des données dans le marketing. *Journal of the Academy of Marketing Science, 45*(2), 135-155. https://doi.org/10.1007/s11747-016-0495-4

Mason, J. (2018). *Recherche qualitative.* Sage Publications.

Mayoh, J., &Onwuegbuzie, A. J. (2015). Vers une conceptualisation des méthodes mixtes de recherche phénoménologique. *Journal of Mixed Methods Research, 9,* 91-107. https://doi.org/10.1177/1558689813505358

Mcintosh, M. J. et Morse, J.M. (2015). Situer et construire la diversité dans les entrevues semi-structurées. *Recherche qualitative mondiale en soins infirmiers, 2,* 233339361559767. https://doi.org/10.1177/2333393615597674

McMahon, D., Seaman, S. et Lemley, D. A. (2015). L'adoption de sites Web par des organisations à but non lucratif et l'impact sur la société. *Technology in Society, 42,* 1-8. https://doi.org/10.1016/j.techsoc.2015.01.001

McTate, E. A. et Leffler, J.M. (2017). Diagnostic du trouble perturbateur de dysrégulation de l'humeur : Intégration d'entrevues semi-structurées et non structurées. *Clinical Child Psychology &Psychiatry, 22,* 187-203. https://doi.org/10.1177/1359104516658190

Meisner, M. (2018). Conséquences financières des cyberattaques conduisant à des violations de données dans le secteur de la santé. *Copernican Journal of Finance &Accounting, 6*(3), 63. https://doi.org/10.12775/cjfa.2017.017

Mierzwa, S., et Scott, J. (2017). *Cybersécurité dans les organisations à but non lucratif et non gouvernementales.* Institut de technologie des infrastructures essentielles. https://www.researchgate.net/publication/314096686_Cybersecurity_in_Non-Profit_and_Non-Governmental_Organizations

Mingers, J. et Standing, C. (2018). Qu'est-ce que l'information? vers une théorie de l'information objective et véridique. *Journal of Information Technology, 33(2),* 85-104. https://doi.org/10.1057/s41265-017-0038-6

Mittal, S., Durak, U., &Ören, T. I. (2017). *Guide des disciplines basées sur la simulation : Faire progresser notre avenir informatique*. Springer.

Mohajan, H. K. (2018). Méthodologie de recherche qualitative en sciences sociales et matières connexes. *Journal of Economic Development, Environment and People, 7*(1), 23-48. https://doi.org/10.26458/jedep.v7i1.571

Mohammed, S., Ramkumar, L., &Rajasekar, V. R. (2017). Authentification par mot de passe dans la sécurité informatique: Pourquoi est-elle toujours là? *The SIJ Transactions on Computer Science Engineering &its Applications (CSEA), 5*(2), 33-36. https://www.researchgate.net/publication/316350564_Password-based_Authentication_in_Computer_Security_Why_is_it_still_there

Monov, L.B., &Karev, M. L. (2018). Cadre conceptuel de la guerre de l'information. International *Journal of Recent Scientific Research, 9*(5F), 26859-26866. https://doi.org/10.24327/IJRSR

Moore, B., Calvo-Amodio, J. et Junker, J. (2017). L'application d'un travail de prévention de l'omplementarisme permet d'appliquer dessolutionsaux ervice organisations à uneé de susable holistic management model. *Systemic Practice &Action Research, 30*(5), 487-513. https://doi.org/10.1007/s11213-016-9403-6

Morgan, S. J., Pullon, S. R., Macdonald, L.M., McKinlay, E.M., &Gray, B. V. (2017). Étude de cas recherche observationnelle : Un cadre pour mener des études de cas où les données d'observation sont au centre de l'attention. *Qualitative Health Research, 27(7),* 1060-1068. https://doi.org/10.1177/1049732316649160

Morris, N. S., &Rosenbloom, D. A. (2017). Définir et comprendre les études pilotes et autres études de faisabilité. *American Journal of Nursing, 117*,38-47. https://doi.org/10.1097/01.NAJ.0000513261.75366.37

Moskal, S., Yang, S. J., &Kuhl, M. E. (2018). Évaluation des cybermenaces via la simulation de scénarios d'attaque à l'aide d'une approche intégrée de

modélisation de l'adversaire et du réseau. *Journal of Defense Modeling and Simulation, 15*(1), 13-29. https://doi.org/10.1177/1548512917725408

Mowlana, H. (2019). Human communication theory: A five-dimensional model. *Journal of International Communication*, *25*(1), 3-33. https://doi.org/10.1080/13216597.2018.1560351

Muegge, S., &Craigen, D. (2015). Une approche scientifique de la conception pour construire des infrastructures essentielles et communiquer les risques liés à la cybersécurité. *Technology Innovation Management Review*, *5*(6), 6-16. https://search.proquest.com/docview/1697867587?accountid=45049

Muhammad, B. F. (2018). A review of Gadamerian and Ricoeurian hermeneutics and its application to interpretive accounting research. *Qualitative Research in Organizations and Management*, *13*(3), 261-283. https://doi.org/10.1108/QROM-07-2017-1550

Commission nationale pour la protection des sujets humains de recherche biomédicale et comportementale. (1979). Le rapport Belmont : Principes éthiques et lignes directrices pour la protection des sujets humains de recherche. Washington, DC: U.S. Department of Health and Human Services.

Conseil national des organisations à but non lucratif. (2016). Impact économique. https://www.councilofnonprofits.org/economic-impact

Newton, V. L. (2017). « C'est bien de pouvoir parler »: Une exploration des complexités des relations entre les participants et les chercheurs lors de la conduite de

recherches sensibles. *Womens Studies International Forum, 61*,93-99. https://doi.org/10.1016/j.wsif.2016.11.011

Ngongo, C. J., Frick, K. D., Hightower, A. W., Mathingau, F. A., Burke, H., &Breiman, R. F. (2015). Les perils de straying de protocol: Échantillonnage biaset interviewer effects. *PLoS ONE, 10*(2), 1-11. https://doi.org/10.1371/journal.pone.0118025

Nieuwenhuis, L. J.M., Ehrenhard, M. L., &Prause, L. (2018). Le passage au cloud computing : l'impact des technologies perturbatrices sur l'écosystème commercial des logiciels d'entreprise. *Technological Forecasting and Social Change, 129*,308. https://search.proquest.com/docview/2084459733?accountid=45049

Nikolić, D. (2015). Practopoïèse: Ou comment la vie favorise un esprit. *Journal of Theoretical Biology, 373*, 40-61. https://doi.org/10.1016/j.jtbi.2015.03.003

Noble, H., &Smith, J. (2015). Questions de validité et de fiabilité dans la recherche qualitative. *Evidence Based Nursing, 18*(2), 34-35. https://doi.org/10.1136/eb-2015-102054

Nowell, L. S., Norris, J.M., White, D. E., &Moules, N. J. (2017). Analyse thématique : S'efforcer de répondre aux critères de fiabilité. *International Journal of Qualitative Methods, 16,* 1-13. https://doi.org/10.1177/1609406917733847

Oakley, J. G. (2019). La state de modern offensive security. *Professional Red Teaming*, 29-41. https://doi.org/10.1007/978-1-4842-4309-1_3

Ogliastri, E., Jäger, U. P., &Prado, A.M. (2016). Stratégie et structure dans les organisations à but non lucratif hautement performantes: Aperçus de cas

Iberoamerican. *Voluntas, 27*(1), 222-248. https://doi.org/10.1007/s11266-015-9560-8

Pandey, S., &Chawla, D. (2016). Utiliser la recherche qualitative pour établir la validité du contenu des constructions de style de vie électronique et de qualité du site Web. *Qualitative Market Research, 19*(3), 339-356. https://doi.org/10.1108/QMR-05-2015-0033

Pardini, D. J., Heinisch, A.M., &Parreiras, F. S. (2017). Gouvernance et gestion de la cybersécurité pour les réseaux intelligents dans les services publics d'énergie brésiliens. *Journal of Information Systems and Technology Management, 14*(3), 385-400. https://doi.org/10.4301/s1807-17752017000300006

Park, W., Na, O., &Chang, H. (2016). Une recherche exploratoire sur la conception avancée de la sécurité des médias intelligents pour un système d'information sur le renseignement durable. *Multimedia Tools and Applications, 75*(11), 6059-6070. https://doi.org/10.1007/s11042-014-2393-4

Parks, R., Xu, H., Chu, C. H., et Lowry, P.B. (2017). Examiner les conséquences prévues et imprévues des mesures de protection de la vie privée de l'organisation. *European Journal of Information Systems, 26*(1), 37-65. https://doi.org/10.1057/s41303-016-0001-6

Pascalev, M. (2017). Échanges de renseignements personnels : Rétablir le consentement à l'autogestion de la protection de la vie privée. *Ethics and Information Technology, 19*(1), 39-48.

Pearce, G. (2017). Gouvernance, risque, conformité et étude de cas big data. *ISACA Journal, 6,* 1-7.

Pelosi, L. (2015). Le participant en tant que protagoniste en évolution. *Qualitative Research Journal, 15*(2), 112-120. https://doi.org/10.1108/qrj-01-2015-0003

Pillay, K. (2017). Introduction de l'éditeur invité: AJIC focus section on cybersecurity. *African Journal of Information and Communication, 20,* 79–82. https://doi.org/10.23962/10539/23575

Posey, C., Raja, U., Crossler, R. E., &Burns, A. J. (2017). Faire le point sur la protection de la vie privée des organisations: Catégoriser et évaluer les menaces pesant sur les informations personnellement identifiables aux*États-Unis. European Journal of Information Systems, 26*(6), 585-604. https://doi.org/10.1057/s41303-017-0065-y

Pouloudi, N., Currie, W., &Whitley, E. A. (2016). Entangled stakeholder roles and perceptions in health information systems: A longitudinal study of the U.K. NHS N3 network. *Journal of the Association for Information Systems, 17*(2), 107-161. https://doi.org/10.17705/1jais.00421

Prakash, M., &Singaravel, G. (2015). Une approche pour la prévention des atteintes à la vie privée et des fuites d'informations dans l'exploration de données sensibles. *Ordinateurs et génie électrique, 45,* 134-140. https://doi.org/10.1016/j.compeleceng.2015.01.016

Preiser, R., Biggs, R., De Vos, A., &Folke, C. (2018). Social-ecological systems as complex adaptive systems: organizing principles for advancing research methods

and approaches. *Ecology and Society*, (4), 46. https://doi.org/10.5751/ES-10558-230446

Proctor, R. W., &Xiong, A. (2018). L'adoption de méthodes statistiques au niveau de la population a transformé la science psychologique, mais pour le mieux: Commentaire sur Lamiell. *American Journal of Psychology, 131*(4), 483-487. https://doi.org/10.5406/amerjpsyc.131.4.0483

Qu, S. Q., &Dumay, J. (2011). L'entretien de recherche qualitative. *Qualitative Research in Accounting and Management*, *8*(3), 238-264. https://doi.org/10.1108/11766091111162070

Quinney, L., Dwyer, T., &Chapman, Y. (2016). Qui, où et comment interviewer des pairs. *SAGE Open, 6*(3), 215824401665968. https://doi.org/10.1177/2158244016659688

Quirós, P., Alonso, P., Díaz, I., &Montes, S. (2015). Protection des données : une approche floue. *International Journal of Computer Mathematics*,*92*(9), 1989-2000. https://doi.org/10.1080/00207160.2014.928700

Rainie, S., Schultz, J., Briggs, E., Riggs, P., et Palmanteer-Holder, N. L. (2017). Data as a strategic resource: self-determination, governance, and the data challenge for indigenous nations in the United States. *International Indigenous Policy Journal, 8,* https://doi,org/10.18584/iipj.2017.8.2.1

Rajendran, K., Jayabalan, M., &Rana, M. E. (2017). Un tudysur k-anonymat, l-diversité, et t-proximité techniques se concentrant medical data. I*nternational Journal of Computer Science and Network Security, 17*(12), 172-177.

https://www.researchgate.net/publication/322330948_A_Study_on_k-anonymity_l-diversity_and_t-closeness_Techniques_focusing_Medical_Data

Ranney, M. L., Meisel, Z. F., Choo, E. K., Garro, A.C., Sasson, C., et Morrow Guthrie, K. (2015). La recherche sur l'estiction de données, la nalyse et la recherchesur l'esults sont part II: la recherchesur lesdonnées, lanalyse et larecherche sur lesrésultats. *Academic emergency medicine: official journal of the Society for Academic Emergency Medicine*, *22*(9), 1103-1112. https://doi.org/10.1111/acem.12735

Rathi, D., &Given, L.M. (2017). L'utilisation par les organisations à but non lucratif d'outils et de technologies pour la gestion des connaissances : une étude comparative. *Journal of Knowledge Management, 21*(4), 718-740. https://doi.org/10.1108/JKM-06-2016-0229

Reddy, A. G., Das, A. K., Odelu, V., &Yoo, K.-Y. (2016). Une authentification biométrique améliorée avec protocole d'accord de clé pour une architecture multiserveur basée sur la cryptographie à courbe elliptique. *PLoS ONE*, *11*(5), 1-28. https://doi.org/10.1371/journal.pone.0154308

Ridder, H. (2017). The theory contribution of case study research designs. *Business Research*, *10*(2), 281-305. https://doi.org/10.1007/s40685-017-0045-z

Roberts, K., Dowell, A., &Nie, J. (2019). Tenter de faire preuve de rigueur et de reproductibilité dans l'analyse thématique des données de recherche qualitative; une étude de cas sur le développement de livres de codes. *Méthodologie de recherche médicale*BMC, *19*(1). doi:10.1186/s12874-019-0707-y

Robins, C. S., &Eisen, K. (2017). Stratégies pour l'utilisation efficace de NVivo dans une étude à grande échelle: Analyse qualitative et abrogation de ne pas demander, ne pas dire. *Enquête qualitative, 23*(10), 768-778. https://doi.org/10.1177/1077800417731089

Rogers, R. W. (1975). Une protection motivation theory de fear appeals et unettitude change1. *Journal of Psychology, 91*(1), 93-114. https://doi.org/10.1080/00223980.1975.9915803

Romanosky, S. (2016). Examiner les coûts et les causes des cyberincidents. *Journal of Cybersecurity, 2*(2), 121-135. https://doi.org/10.1093/cybsec/tyw001

Rossouw, c. S., &Willett, M. (2017). Assurance de l'infonuagique – Examen des lignes directrices de la littérature. *Information and Computer Security, 25*(1), 26-46. https://doi.org/10.1108/ICS-09-2015-0037

Rousseau, D. (2015). S ystems theory: Son present et potential. *Systems Research and Behavioral Science, 32*(5), 522-533. https://doi.org/10.1002/sres.2354

Rousseau, D., Wilby, J., Billingham, J., &Blachfellner, S. (2018). *Systemologie Générale : Transdisciplinarité pour la découverte, la perspicacité et l'innovation.* Springer.

Samani, A., Ghenniwa, H. H., et Wahaishi, A. (2015) (2015). La protection de la vie privée dans l'Internet des objets : un modèle et un cadre de protection. *Procedia Computer Science, 52,* 606-613. https://doi.org/10.1016/j.procs.2015.05.046

Sarabi, A., Naghizadeh, P., Liu, Y., &Liu, M. (2016). Entreprise risquée : prédiction fine des violations de données à l'aide de profils d'entreprise. *Journal of Cybersecurity, 2*(1), 15-28. https://doi.org/10.1093/cybsec/tyw004

Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., Burroughs, H.C., Jinks, C. (2018). Saturation dans la recherche qualitative : Explorer sa conceptualisation et son opérationnalisation. *Quality and Quantity, 52*(4), 1893-1907. https://doi.org/10.1007/s11135-017-0574-8

Schneider, A., Wickert, C., et Marti, E. (2016). Réduire la complexité en créant de la complexité : une perspective de théorie des systèmes sur la façon dont les organisations réagissent à leurs environnements. *Journal of Management Studies*, *54*(2), 182-208. https://doi.org/10.1111/joms.12206

Sen, R., &Borle, S. (2015). Estimation de la contextuelle risk de data bportée: An empirical approach. *Journal of Management Information Systems, 32*(2) 314-341. https://doi.org/10.1080/07421222.2015.1063315

Shapiro, Y. (2015). Dynamical Systems Therapy (DST): Théorie et applications pratiques. *Psychanalytic Dialogues, 25*(1), 83-107. https://doi.org/10.1080/10481885.2015.991245

Shukla, T. (2016). Une introduction à la recherche qualitative. *South Asian Journal of Management, 23*(4), 200-202. https://search.proquest.com/docview/1876464111?accountid=45049

Snelson, C. L. (2016). Recherche qualitativeet qualitative et éthique de l'information:vue d'ensemble de l'itérature. *International Journal of Qualitative Methods,* 15(1), 1-15. https://doi.org/10.1177/1609406915624574

Sommestad, T., Karlzén, H., &Hallberg, J. (2015). La suffisance de la théorie du comportement planifié pour expliquer la conformité à la stratégie de sécurité de

l'information. *Information and Computer Security, 23*(2), 200-217. https://doi.org/10.1108/ICS-04-2014-0025

Stacey, A. (2016). Militating against data fabrication and falsification: A protocol of trias politica for business research. *Electronic Journal of Business Research Methods, 14*(2), 72-82. https://academic-publishing.org/index.php/ejbrm/article/view/1343/1306

Stewart, H., &Jürjens, J. (2017). Gestion de la sécurité de l'information et aspect humain dans les organisations. *Information and Computer Security, 25*(5), 494-534. https://doi.org/10.1108/ICS-07-2016-0054

Tahir, R. (2018). Une étude sur les logiciels malveillants et les techniques de détection des logiciels malveillants. *International Journal of Education and Management Engineering, 8*(2), 20. https://doi.org/10.5815/ijeme.2018.02.03

Teixeira, B., Gregory, P. A., et Austin, Z. (2017). Comment les pharmaciens de l'Ontario s'adaptent-ils à l'évolution de la pratique? Résultats d'une analyse qualitative utilisant le modèle de gestion du changement de Kotter. *Revue des Pharmaciens du Canada / Canadian Pharmacists*Journal, *150*(3), 198-205. https://doi.org/10.1177/1715163517701470

Theofanidis, D., &Fountouki, A. (2019). Limites et délimitations dans le processus de recherche. *Perioperative Nursing, 7*(3), 155-162. https://doi.org/10.5281/zenodo.2552022

Theophanidis, P., Thibault, G., &Trudel, D. (2017). En marge de la cybernétique. Revue *canadienne des communications*, *42*(3), 397-405. https://doi.org/10.22230/cjc.2017v42n3e3304

Thistoll, T., Hooper, V., &Pauleen, D. J. (2016). Acquérir et développer une sensibilité théorique en entreprenant une revue de la littérature préliminaire fondée. *Qualité et quantité*, *50*(2), 619-636. https://doi.org/10.1007/s11135-015-0167-3

Törmänen, J., Hämäläinen, R. P., &Saarinen, E. (2016). Inventaire de l'intelligence des systèmes. *Learning Organization*, *23*(4), 218-231. https://doi.org/10.1108/TLO-01-2016-0006

Tumbas, S., Berente, N., &vom Brocke, J. (2018). Innovation numérique et entrepreneuriat institutionnel: perspectives principales deleur rôle émergent. *Journal of Information Technology (Palgrave Macmillan)*, 33(3), 188-202. https://doi.org/10.1057/s41265-018-0055-0

Turner, J. R. et Baker, R.M. (2019). Complexité: un point devueavec des pplications p otential pour les sciences occiales. *Systèmes*, *7*(1), 4. https://doi.org/10.3390/systems7010004

Van de Pas, J., &van Bussel, G. (2015). « Vie privée perdue - et retrouvée? » La chaîne de valeur de l'information comme modèle pour répondre aux préoccupations des citoyens. *The Electronic Journal Information Systems Evaluation*, *18*(2), 185-195.

Van den Berg, A., &Struwig, M. (2017). Lignes directrices à l'intention des chercheurs qui utilisent une approche de recherche qualitative consensuelle adaptée dans la

recherche en gestion. *Electronic Journal of Business Research Methods*,15(2). https://search. proquest-com.ezp.waldenulibrary.org/abicomplete/docview/1954333307/BB8F784768FE42F7PQ/1?accountid=14872

Van Rooy, G., Mufune, P., et Amadhila, E. (2015). Experiences and perceptions of barriers to health services for elderly in rural Namibia: A qualitative study. *SAGE Open, 5*(3), 1-10. https://doi.org/10.1177/2158244015596049

Venkatesh, V., Brown, S. A., et Sullivan, Y. W. (2016). Guidelines for conducting mixed-methods research: An extension and illustration. *Journal of the Association for Information Systems, 17*(7), 435-494. https://search.proquest.com/docview/1813158448?accountid=45049

Verhoeff, R. P., Knippels, M. P. J., Gilissen, M. G. R., et Boersma, K. T. (2018). La nature théorique de la pensée systémique. Perspectives on systems thinking in biology education. *Frontières dans l'éducation*. https://doi.org/10.3389/feduc.2018.00040

par rapport à la pratique dans les études publiées à l'aide d'ATLAS et de NVivo, 1994-2013. *Vie sociale*

par Bertalanffy, L. (1968). General systems theory as integrating factor in contemporary science. *Actes de XIV Congrès International Pour la Philosophie, 2,* 335-340. https://doi.org/10.5840/wcp1419682120

von Bertalanffy, L. (1972). The History and Status of General Systems Theory. *Academy of Management Journal, 15*(4), 407-426. https://doi.org/10.2307/255139

Wallace, M. et Sheldon, N. (2015). Éthique de la recherche commerciale : Points de vue des observateurs participants : JBE JBE. *Journal of Business Ethics, 128*(2), 267-277. https://doi.org/10.1007/s10551-014-2102-2

Wardale, D., Cameron, R., &Li, J. (2015). Considérations relatives à la recherche multidisciplinaire, adaptée à la culture et aux méthodes mixtes. *Electronic Journal of Business Research Methods, 13*(1), 37-47. https://www.semanticscholar.org/paper/Considerations-for-multidisciplinary%2C-culturellement-Wardale-Cameron/a42467f63a41ac1d780769d2e5bb0e635e70df47

Wels, H. (2015). « Animaux comme nous »: Revisiter l'ethnographie organisationnelle et la recherche. *Journal of Organizational Ethnography, 4*(3), 242-259. https://doi.org/10.1108/JOE-12-2014-0039

Werder, K., &Maedche, A. (2018). Expliquer l'émergence de l'agilité d'équipe : une perspective complexe de systèmes adaptatifs. *Technologies de l'information et personnes, 31*(3), 819. http://search.ebscohost.com/login.aspx?direct=true&db=edb&AN=129756201&site=eds-live

Williams, P. A. et Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. *Medical devices (Auckland, N.Z.), 8,* 305-16.

Williams, T. L., et Needham, C. R. (2016). Transformation de l'a c ité: l'influence de la gentrification sur le centre commercial business owners de Harlem, New York.

Sage Open, *6*(4), 2158244016673631. https://doi.org/10.1177/2158244016673631

Wolgemuth, J. R., Hicks, T., &Agosto, V. (2017). Déballage d'unessumptions dans research synthesis: Un critical construct synthesis unpproach. *Educational Researcher*, *46*(3), 131-139. https://doi.org/10.3102/0013189X17703946

Wong, T. S., Gaston, A., DeJesus, S., &Prapavessis, H. (2016). L'utilité d'un cadre de théorie de la motivation de protection pour comprendre le comportement sédentaire. *Health Psychology and Behavioral Medicine*, *4*(1), 29-48. https://doi.org/10.1080/21642850.2015.1128333

Woods, M., Paulus, T., Atkins, D. P., &Macklin, R. (2016). Faire progresser la recherche qualitative à l'aide d'un logiciel d'analyse de données qualitatives (QDAS)? Examen du potentiel par rapport à la pratique dans les études publiées à l'aide d'ATLAS. ti et NVivo, 1994-2013. *Social Science Computer Review*, 34(5), 597-617.

Woszczynski, A.B., &Green, A. (2017). Résultats d'apprentissage pour les compétitions de cyberdéfense. *Journal of Information Systems Education*, *28*(1), 21-41.

Wright, R. T., Roberts, N., et Wilson, D. (2017). Le rôle du contexte dans l'assimilation informatique: Une étude multi-méthodes d'une plate-forme SaaS dans le secteur à but non lucratif américain. *European Journal of Information Systems*, *26*(5), 509-539. https://doi.org/10.1057/s41303-017-0053-2

Wu, Y. P., Thompson, D., Aroian, K. J., Mcquaid, E. L., et Deatrick, J. A. (2016). Commentaire : Rédaction et évaluation des rapports de recherche qualitative.

Journal of Pediatric Psychology, 41(5), 493-505. https://doi.org/10.1093/jpepsy/jsw032

Xu, X., Wang, B., &Zhou, Y. (2016). Méthode basée sur un modèle de confiance pour la prise de décision en grand groupe avec des informations de préférence incomplètes. *Journal of Intelligent &Fuzzy Systems, 30*(6), 3551–3565. https://doi.org/10.3233/ifs-162100

Yang, Y., Pankow, J., Swan, H., Willett, J., Shannon, G.M., Rudes, D. S., &Knight, K. (2018). Préparation à l'analyse : Guide pratique d'une étape critique pour la rigueur procédurale dans les études de recherche qualitative multisite à grande échelle. *Qualité et quantité, 52*(2), 815-828. https://doi.org/10.1007/s11135-017-0490-y

Yang, L., Li, J., Elisa, N., Prickett, T., &Chao, F. (2019). Vers une gouvernance big data en cybersécurité. *Découverte et applications compatibles avec les données, 3*(1). https://doi.org/10.1007/s41688-019-0034-9

Yeong Kim, H., &Suh Cho, J. (2018). Cadre de gouvernance des données pour la mise en œuvre de big data avec analyse de cas NPS en Corée. *Journal of Business &Retail Management Research, 12*(03). 36 à 45. https://doi.org/10.24052/jbrmr/v12is03/art-04

Yin, R. K. (2017). *Études de cas et applications : Conception et méthodes*. SAGE.---

Yost, J. R. (2016). The march of IDES: Early history of Intrusion-Detection Expert Systems. *IEEE Annals of the History of Computing, 38*(4), 42-54. https://doi.org/10.1109/MAHC.2015.41

Young, J.C., Rose, D.C., Mumby, H. S., Benitez-Capistros, F., Derrick, C. J., Finch, T., Garcia, C., Home, C., Marwaha, E., Morgans, C., Parkinson, S., Shah, J., Wilson, K. A., &Mukherjee, N. (2018). Un guide méthodologique sur l'utilisation et la production de rapports sur les entrevues dans la recherche en sciences de la conservation. *Methods in Ecology and Evolution, 9*(1), 10-19. https://doi.org/10.1111/2041-210x.12828

Young, N., &Drees, R. (2018). Cybersécurité pour les équipements de test automatique. *IEEE Instrumentation &Measurement Magazine, 21*(4), 4-8. https://doi.org/10.1109/MIM.2018.8423738

Zafar, H., Ko, M. S., &Osei-Bryson, K.-M. (2016). La valeur du DPI au sein de l'équipe de direction supérieure sur le rendement en cas d'atteintes à la sécurité de l'information. *Information Systems Frontiers, 18*(6), 1205-1215. https://doi.org/10.1007/s10796-015-9562-5

Zhang, X., Yuan, Y., Zhou, Z., Li, S., Qi, L., &Puthal, D. (2019). Détection et prévention des intrusions dans le cloud, le brouillard et l'Internet des objets. *Réseau de sécurité et de communication,* 2019(4529957), 1-4.

Annexe : Protocole d'entrevue

Projet : Doctorat en technologie de l'information de l'Université Walden

Type d'entrevue :_____

Date:_____

Lieu:_____

Intervieweur:_____

Personne

interrogée :_____

Titre du poste de la personne

interviewée :_____

[Expliquer le projet en clarifiant a) le but de l'étude, b) plusieurs sources de collecte de données, c) la confidentialité des données et d) la conclusion de l'entrevue dans un délai de 60 minutes.]

[Donner les coordonnées de la personne interrogée]

[Informer la personne interrogée du formulaire de consentement attendu de tous les participants à l'étude et des plans d'enregistrement de l'audio de l'entrevue (fournir une copie si nécessaire).]

[Testez la fonctionnalité de l'enregistreur audio numérique. Confirmer si le participant accepte l'enregistrement de la session]

Questions d'entrevue :

1. Comment évaluez-vous les atteintes à la protection des données dans votre organisation, en ce qui concerne le fait que l'organisation réussisse à les contenir ou qu'elle échappe à tout contrôle?

2. Entre les violations de données internes et externes, lesquelles affectent le plus votre organisation et pourquoi?

3. Quelles stratégies utilisez-vous pour vous assurer que votre personnel informatique est qualifié pour traiter les failles de sécurité ? Pourquoi ou pourquoi pas.

4. Quelles stratégies employez-vous pour assurer des budgets adéquats à votre service informatique afin de traiter les atteintes à la protection des données? Pourquoi ou pourquoi pas?département pour traiter les atteintes à la protection des données? Pourquoi ou pourquoi pas ?

5. Expliquez si votre organisation sensibilise les employés à la sécurité au moyen de programmes spéciaux mis en œuvre par le gestionnaire des SI?

6. Quelles procédures votre organisation met-elle en œuvre pour effectuer des audits de conformité internes dans le cadre des stratégies utilisées pour protéger les informations contre les cyberattaques?

7. Quels processus de sécurité des données votre organisation met-elle en œuvre pour se protéger contre tout accès non autorisé aux réseaux de l'organisation ?

8. À quelle fréquence votre organisation forme-t-elle son personnel sur les pratiques exemplaires en matière de sécurité des TI? Pensez-vous que c'est suffisant et pourquoi?

9. Quelle est l'étendue de l'automatisation des processus dans votre organisation en ce qui concerne les stratégies utilisées pour protéger les informations contre les cyberattaques?

10. À quelle fréquence votre organisation rejette-t-elle périodiquement les renseignements personnels à sa disposition dont elle n'a plus besoin dans le cadre de sa stratégie de protection des renseignements contre les cyberattaques?

11. Quelles sont les procédures adoptées par votre organisation pour éliminer les renseignements personnels qui ne sont plus nécessaires, pour protéger les renseignements contre les cyberattaques?

12. Selon vous, quelles stratégies votre organisation devrait-elle adopter pour améliorer la sécurité des TI?

[Exprimer sa gratitude aux personnes interrogées pour leur participation et leur aide à l'entrevue. Reformulez l'obscurité de l'étude à l'égard des répondants et de leurs réponses. Avisez la personne interrogée que vous lui fournirez la copie du fichier de transcription aux fins d'évaluation, de consentement et de retour].