

Gestion et perception des risques cyber par le dirigeant de PME

Laure Zordan

Université de Montpellier, UR Montpellier Research in Management, Montpellier Management (MOMA), Espace Richter Rue Vendémiaire Bât B, 34000 Montpellier, France
laurezordan@outlook.fr

Julien Granata

Montpellier Business School, Chaire MIND, 34000 Montpellier, France
j.granata@montpellier-bs.com

Estelle Pellegrin-Boucher

Université de Montpellier, UR Montpellier Research in Management, Montpellier Management (MOMA), Espace Richter Rue Vendémiaire Bât B, 34000 Montpellier, France
estelle.boucher@umontpellier.fr

Mots-clés : risque cyber, PME, dirigeant, cybersécurité, systèmes d'information.

Résumé :

Le risque cyber est un risque opérationnel lié à l'atteinte du système d'information. L'augmentation de l'usage du numérique en organisation accentue sa menace et il est souvent sous-estimé par les PME. En tant que leader sur de nombreux projets, le dirigeant de PME fait face à des difficultés pour assurer une gestion du risque cyber optimale. Cette recherche vise ainsi à étudier la question des déterminants qui peuvent influencer le dirigeant de PME dans sa gestion du risque cyber. Pour y répondre, nous avons analysé l'influence des déterminants internes à la PME, l'influence des déterminants psychologiques propres au dirigeant, ainsi que l'influence des déterminants externes sur la gestion du risque cyber par le dirigeant. Nous avons déployé un protocole de recherche qualitative fondé sur 22 entretiens semi-directifs avec des dirigeants de PME ainsi qu'avec des professionnels du secteur de la cybersécurité. Les résultats de la recherche confirment certains déterminants déjà portés par la littérature comme l'influence de la taille de l'entreprise sur la gestion du risque cyber par le dirigeant ou encore le poids de plus en plus important des déterminants économiques, réglementaires et réputationnels. Néanmoins, la recherche apporte deux nouveaux déterminants qui influencent le dirigeant : la proximité avec le risque cyber (influence positive) et les sentiments de peur et d'incompétence qui peuvent conduire à l'évitement (influence négative).

1. Introduction

Les menaces qui émanent du cyberspace ainsi que le risque cyber sont devenus ces dernières années des enjeux de grande ampleur concernant tous les acteurs de l'économie (Ventre, 2016). Les menaces informatiques qui visent l'information sont en effet omniprésentes et leurs origines sont variées, par exemple, elles peuvent provenir d'employés actuels ou anciens de l'entreprise, de pirates informatiques, d'auteurs de virus ou d'attaques informatiques, de personnes liées à l'espionnage commercial, etc. (Dutta et McCrohan, 2002). Ce risque concerne également les Petites et Moyennes Entreprises (PME) car le dernier rapport de la menace informatique publié par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI, 2022) montre qu'en 2021, 34% des victimes de ransomwares étaient des TPE, PME et ETI. La principale raison de ces attaques est que les PME possèdent des moyens de défense inférieurs à ceux des grandes entreprises (Barlette, Gundolf et Jaouen, 2017). Par ailleurs, nombreuses sont les PME qui pensent ne pas être vulnérables au risque cyber, particulièrement en raison de leur petite taille et de leur nombre d'actifs limité (Prnewswire, 2015). Pourtant, ces risques informatiques peuvent engendrer des crises menant à la faillite des nombreuses PME qui en sont ciblées (Oppens, 2020) et qui doivent mettre en place des stratégies spécifiques à ce type d'entreprise.

La littérature portant sur les PME met en effet en lumière des caractéristiques propres à cette catégorie d'entreprises, telles que le rôle majeur de l'intuition dans la prise de décision stratégique des dirigeants, mais aussi le rôle de l'expérience et de l'affect (Julien, 1990 ; Zacca, Dayan et Elbanna, 2017). Certains travaux soulignent également le manque de ressources, une moins forte hiérarchie et formalisation que dans les grandes entreprises, avec beaucoup de communication orale et implicite, ainsi qu'une vision stratégique basée sur le court terme (Julien, 1990 ; Mintzberg, 1989). Au sujet de la gestion du risque cyber, la littérature confirme ces caractéristiques puisqu'elle montre que les PME possèdent des ressources limitées pour assurer efficacement la sécurité du système d'information (SSI), que ce soit dû à un manque de temps, d'argent, ou d'autres tâches prioritaires à traiter (Gupta et Hammond, 2005 ; Heidt, Gerlach et Buxmann, 2019).

La cybersécurité est devenue une compétence critique et indispensable dont dépend la survie de l'organisation (Chatterjee, 2019). Les compétences spécialisées en cybersécurité et les budgets alloués à ce domaine, tous deux inadéquats, permettent notamment d'expliquer que les PME présentent une gestion du risque cyber limitée (Howard, 2018 ; Stasiak, 2018). Or, très peu de travaux étudient la vision et le rôle des dirigeants concernant la gestion du risque cyber, en particulier dans un contexte de PME (Barlette, 2012 ; Lee et Larsen, 2009 ; Zwikael, 2008). La rareté de ces travaux contraste avec le fait que les PME représentent plus de 99% des entreprises françaises (INSEE, 2021), elles ont donc un poids économique très important. De plus, le comportement du dirigeant de PME doit y être considéré en détail, car il présente des spécificités par rapport au dirigeant de grandes entreprises (Cragg, Caldeir et Ward, 2011). Il serait notamment intéressant de découvrir quelle est la perception du dirigeant de PME concernant le risque cyber et quels sont les facteurs qui influencent la gestion du risque cyber dans un contexte de PME. Confrontés à la rareté de ces recherches et aux enjeux économiques posés par la question de la cybersécurité en PME, nous avons ainsi essayé de répondre à la question de recherche suivante : quels facteurs peuvent influencer le dirigeant de PME dans sa gestion du risque cyber ? Pour répondre à cette problématique, nous avons mené une recherche sur les perceptions et la gestion du risque cyber par les dirigeants de PME en menant une étude qualitative exploratoire afin de mieux comprendre un sujet encore peu étudié.

2. Revue de la littérature

2.1. Le dirigeant de PME et la gestion du risque cyber

2.1.1. Les spécificités du risque cyber en PME

St-Pierre et Therrien (2007) différencient le risque en tant qu'opportunité, du risque en tant que menace. Lors de cette recherche, nous nous intéresserons au risque en tant que menace qui est souvent associé à l'accroissement de la vulnérabilité de l'entreprise. Ces auteurs rappellent également que le risque est perceptuel. En ce sens, l'évaluation du risque se forme implicitement dans un contexte où l'évaluateur a un rôle significatif dans son appréciation.

La perception d'un risque est un phénomène subjectif lié au jugement de l'individu qui peut dépendre du contexte de la situation, des connaissances, de l'expérience, ou encore de l'influence exercée par des groupes de pressions ou les médias (Kouanbenan, Cadet, Hermand et Muñoz Sastre, 2006). Les travaux concernant la perception s'intéressent souvent à l'analyse de l'impact d'un risque perçu de défaillance sur la gestion de l'entreprise (Claveau, Perez et Serboff ; 2018). La recherche de Claveau *et al.* (2018) montre notamment qu'il existe des écarts entre une situation réelle de risque de défaillance et la perception de ladite situation par le dirigeant de PME. En particulier, le dirigeant peut être conscient de faire face à des difficultés dans le financement de son activité, mais un environnement des affaires favorable l'encouragerait à ne pas percevoir le risque de défaillance en question (comme le risque cyber exploré dans notre étude).

La recherche de Strupczewski (2021, p.6) portant sur la proposition d'une définition complète du risque cyber le définit comme « *un risque opérationnel associé à l'exécution d'activités dans le cyberspace, menaçant les actifs informationnels, les ressources TIC et les actifs technologiques, qui peut causer des dommages matériels aux actifs corporels et incorporels d'une organisation, une interruption d'activité ou une atteinte à la réputation.* ». Le risque cyber est en général sous-estimé par les PME et cela entraîne une augmentation de leur vulnérabilité (Alahmari et Duncan, 2020).

Le risque cyber requiert d'assigner des ressources de sécurité des systèmes d'information en vue de garantir une cybersécurité optimale. L'ANSSI (2022) définit la cybersécurité comme l'« *état recherché pour un système d'information lui permettant de résister à des événements issus du cyberspace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises [...]. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information [...]* ».

Zadeh, Jeyaraj et Biros (2020) identifient quatre types de menaces de cybersécurité :

- Les menaces physiques : agressions, incendies, coupures de courant, documents non détruits, l'humidité, etc.
- Les menaces humaines : espionnage, extorsion, individu malveillant, enregistrement de frappes, phishing, ingénierie sociale, fausse identité, vol, etc.
- Les menaces sur les données et la communication : déni de service, bombe logique, malware, virus, cheval de Troie, menaces sur la confidentialité et l'intégrité des données, etc.

- Les menaces opérationnelles : piratage, refus d'accès au système, personne non autorisée, logiciel espion, fraude, usurpation d'identité, etc.

Germain (2021) montre qu'une stratégie préventive du risque cyber est très importante pour les organisations. Il doit être pris en considération d'un point de vue stratégique et appréhendé au plus haut niveau d'importance, notamment car la transformation digitale globale en cours de la société ne peut être une réussite sans un investissement initial dans la cybersécurité.

2.1.2 Le rôle du dirigeant dans la gestion du risque cyber

La majorité des déterminants liés à la gestion du risque cyber sont liés à des problématiques managériales (Rainer, Marshall, Knapp et Montgomery ; 2007). Dans un contexte de PME, le dirigeant est souvent le seul décisionnaire en ce qui concerne les décisions stratégiques (Birley, 1982 ; Zacca *et al.*, 2017) et notamment en matière de SSI où il a un fort impact (Barlette, Gundolf et Jaouen, 2017 ; Barton *et al.*, 2016 ; Thong, 1999). Néanmoins, il est souvent seul et n'a pas les compétences adéquates pour identifier et atténuer les risques cyber, ce qui l'amène à renoncer à la gestion de la cybersécurité (Barlette, 2012 ; Njenga et Jordaan, 2016 ; Rainer *et al.*, 2007). Le dirigeant de PME n'a pas suffisamment conscience des problèmes liés au risque cyber (Dojkovski, Lichtenstein, et Warren, 2006 ; Njenga et Jordaan, 2016). Pourtant, son implication est indispensable dans la mise en place, le maintien et la réussite des actions de SSI (Johnston et Hale, 2009).

Par ailleurs, c'est le dirigeant qui est responsable de la politique de SSI dans l'organisation et du respect de la réglementation (Boss, Kirsch, Angermeier, Shingler, Boss ; 2009). Pourtant et en dépit de l'importance de cette responsabilité, le dirigeant est porté vers ses préoccupations au jour le jour et ne définit pas systématiquement une politique de SSI pour son entreprise (Gupta et Hammond, 2005). Le dirigeant de PME a des difficultés à investir dans la SSI car il ne peut associer les dépenses en sécurité avec d'éventuels bénéfices (Dutta et McCrohan, 2002), il doit souvent arbitrer entre son niveau de risque cyber perçu et les budgets alloués à la SSI (Gupta et Hammond, 2005 ; Taylor et Brice, 2012). En conséquence, ces investissements sont souvent biaisés et les données mal sécurisées (Rainer *et al.*, 2007).

De plus, en situation d'urgence, Abaaoukide et Bentaleb (2011) montrent que le manque d'expérience, la non-hiérarchisation des priorités, la recherche d'informations non optimale ainsi qu'un manque de réflexion peuvent engendrer la prise de mauvaises décisions par le dirigeant, notamment en matière de cybersécurité. Le dirigeant peut également prendre des décisions erronées entraînant une augmentation du risque de sécurité sur l'information (Njenga et Jordaan, 2016), ce qui augmente le risque de failles de sécurité (Williams, 2007). Dans l'environnement complexe de la cybersécurité, les risques sont souvent incertains et amènent les individus à se fier à l'affect plutôt qu'à l'évaluation objective des risques (Van Schaik, Renaud, Wilson, Jansen et Onibokun ; 2020). Cette perception des risques influence notamment l'adoption de comportements de cybersécurité (Van Schaik, Jansen, Onibokun, Camp et Kusev ; 2018).

2.2 Les éléments qui influencent la perception des dirigeants et la gestion du risque cyber

2.2.1. Une faible perception du risque cyber chez les dirigeants de PME

Le risque cyber peut impacter l'organisation financièrement (Oppens, 2020 ; Strupczewski, 2021 ; Ventre, 2016) car il peut engendrer des dommages matériels corporels (ordinateurs,

serveurs, locaux de l'organisation, etc) ou incorporels (brevets, fonds de commerce, logiciels, etc). De plus, en relevant de la responsabilité civile, une violation de données peut obliger l'organisation à indemniser les dommages causés aux tiers. Une attaque informatique peut avoir d'autres conséquences directes comme les pertes d'exploitation et de données, et indirectes comme des frais de communication interne et externe ou de gestion de crise (Douzet et Héon, 2013). Par ailleurs, le risque cyber peut impacter la réputation de l'organisation et notamment engendrer la perte de confiance des clients et avoir des conséquences commerciales péjoratives (Strupczewski, 2021). Or, malgré ces enjeux économiques et financiers, la littérature montre que les dirigeants de PME ont une faible conscience du risque cyber ce qui les empêche de mettre en place une politique de gestion des risques cyber adaptée (Dojkovski *et al.*, 2006 ; Douzet et Héon, 2013). En effet, le risque cyber est difficile à appréhender et tandis que les Responsables de la Sécurité des Systèmes d'Information (RSSI) sont qualifiés pour y faire face, ce risque n'est pas pris en compte par les dirigeants (Douzet et Héon, 2013). Le dirigeant a pratiquement toujours une perception technique de la SSI et pensent que c'est un sujet qu'il est préférable de déléguer aux RSSI (Ashenden, 2008). Le problème étant qu'en raison du manque de ressources financières des PME, il est souvent difficile de recruter des fonctions dédiées à l'informatique et la SSI (Cragg *et al.*, 2011 ; Prnewswire, 2015). La perception par les décideurs des risques liés à la SSI est anormalement basse comparée à l'ensemble des risques encourus par leur entreprise ; ils sont alors mal préparés à la gestion des risques cyber (Goodhue et Straub, 1991). Stasiak (2018) montre également que le dirigeant de PME ne perçoit pas suffisamment le risque pour justifier l'augmentation de ressources dédiées à la SSI, ce qui l'empêche de passer à l'action.

2.2.2. Les facteurs qui peuvent influencer la gestion du risque cyber

Premièrement, les compétences, les connaissances et les expériences en cybersécurité sont les principaux facteurs d'influence dans les comportements adoptés en cybersécurité (Bada, Sasse et Nurse ; 2015). Lee et Larsen (2009) montrent notamment que l'intention d'adoption de cybersécurité par le dirigeant de PME est influencée positivement par son expertise. En particulier, ces auteurs montrent que l'intention d'adoption du dirigeant expert en systèmes d'information est davantage influencée par l'évaluation de la menace, tandis que celle du non expert est davantage influencée par l'évaluation de l'adaptation.

Deuxièmement, l'entourage professionnel est un facteur important dans la prise en compte de la cybersécurité. Pour son investissement en cybersécurité, le dirigeant de PME va beaucoup être influencé par ses clients, partenaires commerciaux ou encore ses concurrents (Lee et Larsen, 2009). L'influence est d'autant plus importante pour les industries dépendantes de l'informatique. Johnson (2009) explique que les influences externes motivent davantage l'engagement du dirigeant dans la cybersécurité que les influences internes, notamment dû aux pressions des partenaires commerciaux ou la capacité à concurrencer d'autres entreprises.

Troisièmement, le contexte réglementaire joue un rôle majeur en SSI car il oblige les PME à mettre en place des mesures de protection (Mourrain et Leconte, 2019). Cela est notamment le cas pour le règlement général sur la protection des données (RGPD) entré en vigueur en 2018. Tandis que les PME fortement axées sur la sécurité des données pensent que la mise en conformité RGPD est à leur portée, les PME moins axées sur cet enjeu ont des difficultés à la mettre en œuvre (Sirur, Nurse et Webb ; 2018). Les principaux problèmes rencontrés sont l'ampleur de cette réglementation fastidieuse, la non-maîtrise des actions à mettre en place,

ainsi que la difficulté à cartographier leurs réseaux de données. Néanmoins, le levier juridique pourrait être un moyen efficace d'obliger le dirigeant de PME, même non-impliqués en SSI, à mettre en place des actions (Barlette, 2012).

Quatrièmement, Heidt *et al.* (2019), ont montré l'importance des facteurs affectif ainsi qu'expérientiel dans les investissements liés au système d'information, en particulier, le sentiment de peur face à une menace comme le risque cyber. La théorie de Witte (1992) sur l'EPPM (Extended Parallel Process Model) explique comment les individus réagissent face à des situations qui suscitent la peur au travers de l'influence de deux concepts : la menace (gravité ressentie) et l'efficacité (perception de la probabilité de subir la menace). En appliquant l'EPPM dans un contexte de gestion du risque cyber en PME, nous pouvons supposer que plus la menace est perçue comme insignifiante par le dirigeant, et moins il sera motivé à réagir. A l'inverse, les individus avec une menace perçue élevée et une efficacité perçue faible (lorsqu'ils pensent ne pouvoir rien faire face à la menace) ont tendance à ressentir de la peur et vouloir la contrôler avec un évitement défensif, c'est-à-dire en refusant de mettre en œuvre des actions de protection (Witte, 1994). La peur est alors supprimée et l'individu soulagé. Ainsi, nous pouvons supposer que le dirigeant évite l'information pour atténuer sa peur au lieu de mettre en œuvre des mesures de protection pour atténuer la menace. Si l'individu pense être incapable de répondre au risque, cela génère de l'incertitude et le sentiment de peur est amplifié (Nabi et Myrick, 2019). Dans un contexte de comportements de sécurité de l'information, Boss, Galletta, Lowry, Moody et Polak (2015) montrent notamment que la peur est générée à la suite de la menace perçue, et la gravité l'affecte positivement. Ainsi, plus l'individu est conscient qu'il est vulnérable à un risque important et plus sa peur sera éveillée.

3. Méthodologie de la recherche

3.1 Choix de la méthodologie

Afin de répondre à l'objectif de la recherche, nous avons eu recours à une méthode qualitative de type exploratoire qui est particulièrement pertinente lorsque la recherche visée n'est pas encore suffisamment travaillée (Miles, Huberman et Saldana ; 2018), ce qui était le cas ici car très peu de travaux s'intéressent à la cybersécurité dans un contexte de PME.

Nous avons déployé un protocole de recherche qualitative au sein duquel vingt-deux entretiens semi-directifs ont été menés auprès de dirigeants de PME ainsi qu'auprès d'experts du secteur de la cybersécurité, soit en face à face soit en visioconférence (Evrard, Pras et Roux, 2003 ; Miles *et al.*, 2018). Le choix de cette méthode permet notamment de collecter des données discursives qui transposent l'état mental de la cible d'étude. De plus, selon Miles *et al.* (2018), cette méthode permet de catégoriser des discours précisément analysés, en particulier grâce à la prise en compte des circonstances de l'interview.

3.2 Choix de l'échantillon

Le choix de l'échantillon s'est porté vers des structures aux composants délibérément différents conformément aux travaux de Cook et Campbell (1979) qui montrent qu'un petit échantillon peut être représentatif si les profils d'entreprises sont variés. Poursuivant un objectif de compréhension appliqué à la catégorie d'entreprises des PME, nous les avons alors sélectionnées selon leur secteur d'activité, leur nombre d'utilisateurs informatiques, ainsi que la présence ou non d'un service informatique.

A partir de mars 2021 et jusqu'en janvier 2022, la construction de l'échantillon s'est faite par prospection raisonnée et successive par téléphone, par mail (Fortin et Gagnon, 2016), ainsi que par sollicitation sur le réseau social professionnel LinkedIn. 70 dirigeants de PME ont été approchés individuellement et 12 dirigeants soit 17,14% ont répondu favorablement à la demande de participation. 10 des dirigeants d'entreprises sélectionnés gèrent des petites PME (moins de seize utilisateurs informatiques), et deux dirigeants gèrent de plus grandes PME (plus de cent-trente utilisateurs informatiques). Nous avons fait le choix de PME issues de secteurs d'activité nécessitant l'utilisation de l'outil informatique au quotidien. Ainsi, les PME sélectionnées sont issues des secteurs de l'assurance, de la comptabilité, de la mode, de l'architecture, etc. Leurs dirigeants ont alors été interrogés par entretiens semi-directifs soit en présentiel soit en visioconférence pendant une durée variant de 30 à 45mn (voir tableau 1 ci-dessous). Le sujet de la SSI peut être jugé comme indiscret ou sensible par les entreprises (Kotulic et Clark, 2004 ; Straub et Welke, 1998), ce qui explique le refus de participation de la part de certains dirigeants de PME.

Tableau 1 – Liste des entretiens dirigeants de PME

Répondant	Sexe	Secteur d'activité	Nombre d'utilisateurs informatiques	Service informatique	Age de l'entreprise (années)	Durée de l'entretien (minutes)
1	M	Assurances	130	Oui	23	35
2	F	Mode	1	Non	2	30
3	M	Séjours	3	Non	1	35
4	F	Mode	1	Non	1	30
5	M	Sport	16	Non	76	45
6	F	Comptabilité	150	Oui	16	30
7	M	Architecture	5	Non	16	40
8	M	Environnement	5	Non	2	35
9	M	Marketing digital	5	Non	2	30
10	M	BTP	6	Non	6	30
11	F	Automobile	6	Non	9	30
12	M	Assurances	4	Non	12	40

Afin de compléter ces données, des experts en cybersécurité ont également été interrogés. En effet, la littérature montre que la cybersécurité est un sujet peu maîtrisé par les dirigeants de PME. Les experts sélectionnés dans cette recherche possèdent tous une expérience significative commerciale ou technique dans le secteur de cybersécurité (plus de cinq ans minimum), conformément à ce qui est préconisé dans la littérature (Taylor, 2005 ; Pellegrin-Boucher, Le Roy et Gurău ; 2018). Nous avons également vérifié qu'ils aient déjà accompagné des dirigeants de PME. Ces experts exercent leur fonction au sein d'entreprises toutes spécialisées en cybersécurité, soit d'éditeurs en solutions logicielles, de consulting, ou bien de revendeurs

(produits et services). Nous les avons directement contactés par téléphone ou par mail et 10 entretiens semi-directifs en visioconférence entre 30 et 45 minutes ont été menés (voir tableau 2 ci-dessous).

Tableau 2 – Liste des entretiens experts de la cybersécurité

Répondant	Sexe	Fonction	Secteur d'activité	Années d'expérience en cybersécurité	Durée de l'entretien (minutes)
1	M	Chef de produit	Editeur en sécurité web et sensibilisation à la cybersécurité	10	45
2	M	Ingénieur avant-vente	Editeur en sécurité des endpoints	5	35
3	M	Consultant	Cybersécurité et RGPD	25	35
4	M	Consultant/formateur	Cybersécurité	4	35
5	M	Consultant / formateur	Cybersécurité	15	40
6	M	Responsable technique	Revendeur cybersécurité	5	30
7	M	Consultant	Cybersécurité et RGPD	25	45
8	M	Directeur général / directeur produit	Editeur en chiffrement de bout-en-bout	5	35
9	M	Responsable commercial	Editeur en sécurité des endpoints	17	30
10	M	Responsable commercial	Revendeur cybersécurité et RGPD	20	35

En recherche qualitative, une taille d'échantillon minimale est requise pour assurer la validité interne de la recherche et apporter un niveau de confiance satisfaisant dans les résultats. Ainsi, elle a été déterminée par saturation théorique des données en arrêtant les entretiens lorsqu'ils ne fournissaient plus de nouveaux éléments concernant notre recherche (Cook et Campbell, 1979 ; Yin, 2015). En utilisant le principe de saturation, nous avons arrêté le processus après 12 itérations pour les dirigeants de PME et 10 itérations pour les experts de la cybersécurité.

3.3 La collecte des données

La construction du guide d'entretien a été faite grâce à l'identification dans la revue de littérature des thèmes pertinents pour cette recherche, notamment sur la base des travaux suivants. Tout d'abord certains travaux mettent en évidence le déterminant majeur de l'implication du dirigeant dans la gestion du risque cyber (Barlette, 2012 ; Heidt *et al.* 2019 ; Rainer *et al.*, 2007). La littérature montre d'autres déterminants qui peuvent influencer la gestion du risque cyber en organisation comme les impacts économiques (Douzet et Héon, 2013 ; Strupczewski, 2021), les conséquences sur la réputation (Strupczewski, 2021), ou encore l'influence du contexte réglementaire dans la mise en place de mesures de protection (Barlette, 2012 ; Mourrain et Leconte, 2019 ; Sirur *et al.*, 2018). Ensuite, la recherche de Lee et Larsen (2009) met davantage

en exergue l'influence de déterminants externes comme les clients, les partenaires commerciaux, les concurrents ou encore le secteur d'activité. Enfin, nous nous sommes également basés sur des travaux montrant le rôle majeur de déterminants que nous considérons comme psychologiques dans la gestion du risque cyber. Nous pouvons retrouver la perception du risque (Dojkovski *et al.*, 2006 ; Van Schaik *et al.*, 2020), ou encore l'influence des sentiments et particulièrement de la peur (Witte, 1992 ; Nabi et Myrick, 2019).

Concernant les entretiens avec les dirigeants de PME, le guide d'entretien a alors été divisé en trois thèmes, puis en neuf sous-thèmes. Le guide d'entretien des experts de la cybersécurité a quant à lui été divisé en trois thèmes puis sept sous-thèmes.

Tableau 3 – Dictionnaire des thèmes de la grille d'entretien des dirigeants de PME

Thème	Sous-thème 1	Sous-thèmes 2	Code
1. Déterminants internes	1.1 Caractéristiques de l'entreprise	1.1.1 Nombre d'utilisateurs informatiques	CAR_NOM
		1.1.2 Secteur d'activité	CAR_SEC
		1.1.3 Ancienneté	CAR_ANC
	1.2 Gestion de la cybersécurité	1.2.1 Service informatique dédié	GES_SERV
		1.2.2 Dirigeant	GES_DIR
		1.2.3 Salarié-RSSI	GES_SAL
		1.2.4 Prestataire externe	GES_PRES
	1.3 Apports de mesures de cybersécurité en tant que dirigeant	1.3.1 Aucune	APP_AUC
		1.3.2 Minimum requis	APP_MIN
	1.4 Avoir subi une attaque		ATT_SUB
2. Déterminants psychologiques propre au dirigeant	2.1 Perception du risque cyber	1.5.1 Ne sont pas indispensables	CON_PAS
		1.5.2 Ponctuelles	CON_PONC
		2.1.1 Conscience d'être une cible potentielle	PERC_CIB
		2.1.2 Peu d'intérêt pour les pirates informatiques	PERC_INT
		2.1.3 Déterminants économiques	DET_ECO
		2.1.4 Déterminants réputation	DET_REP
		2.1.5 Déterminants réglementation	DET_REG
	2.2 Niveau de cybersécurité perçu de l'entreprise	2.2.1 Confiance envers le service informatique	NIV_CONF
		2.2.2 Conscience de possibilité d'amélioration	NIV_AME
		2.2.3 Basique	NIV_BAS
	2.4 Sentiments	2.4.1 Peur	SENT_PEU

3. Déterminants externes		2.4.2 Incompétence	SENT_INC
		2.4.3 Désintérêt	SENT_DES
		2.4.4 Anxiété	SENT_ANX
		2.4.5 Intéressement	SENT_INT
	3.1 Vecteurs d'influences	3.1.1 Actualité/médias	VEC_ACT
		3.1.2 Webinars	VEC_WEB
		3.1.3 Echanges avec des experts	VEC_EXP
		3.1.4 Réseaux sociaux	VEC_RES
		3.1.5 Entourage	VEC_ENT
		3.1.6 Syndicat professionnel	VEC_SYND
		3.1.7 Aucun	VEC_AUC

Tableau 4 – Dictionnaire des thèmes de la grille d’entretien des experts de la cybersécurité

Thème	Sous-thème 1	Sous-thèmes 2	Code
1. Déterminants internes	1.1 Attractivité des PME pour les pirates informatiques	1.1.1 Cible facile	ATT_CIB
		1.1.2 Volume d’informations insuffisant	ATT_VOL
	1.2 Niveau de cybersécurité des PME	1.2.1 Minimum appliqué	GES_SERV
2. Déterminants propres au dirigeant	2.1 Conscience des risques cyber	2.1.1 Conscience du risque faible	CONS_FAI
	2.2 Niveau de cybersécurité perçu par le dirigeant	2.2.1 Conforme à la réalité	NIV_CONF
		2.2.2 Idéalisé	NIV_IDEA
	2.3 Compétences techniques	2.3.1 Superficielles	COMP_SUP
		2.3.2 Inexistantes	COMP_INE
	2.4 Influence sur la gestion du risque cyber après une attaque informatique	2.4.1 Renforcée	INF_RENF
		2.4.2 Identique	INF_IDEN
		2.4.3 Temporaire	INF_TEMP
3. Déterminants externes	3.1 Vecteurs d’influences sur la perception	3.1.1 Attaque informatique sur PME similaire	VEC_ACT
		3.1.2 Investissement en cybersécurité chez un concurrent	VEC_INVE
		3.1.3 Sentiment de peur	VEC_PEUR
		3.1.4 Subir une attaque informatique	VEC_SUB
		3.1.5 Ignorance	VEC_ING

		3.1.6 Valeurs morales	VEC_MORA
		3.1.7 Entourage direct	VEC_ENTO
		3.1.8 Règlementation	VEC_REG
		3.1.9 Médias	VEC_MED

3.4 L'analyse des données

Les entretiens ont été enregistrés, intégralement retranscrits, codés manuellement puis enrichis avec des verbatims selon les principes de l'analyse de contenu (Miles *et al.*, 2018). L'analyse des données a ainsi reposé sur la méthode de l'analyse de discours fondée sur les différentes thématiques déterminées (Miles *et al.*, 2018). D'abord, nous avons identifié les unités de sens en relevant les mots ou les phrases liées à l'un des thèmes prédéterminés. Puis, nous avons réalisé un comptage d'occurrences pour chaque répondant afin de mesurer le poids de chaque thème dans leurs discours.

Deux matrices ont été construites, l'une dédiée à l'analyse des discours des dirigeants de PME, et l'autre dédiée à celle des experts de la cybersécurité. Ensuite, pour les deux matrices respectives, les thèmes ont été comparés entre eux afin de dégager des similitudes et divergences dans les discours. Cela nous a permis de compléter les thèmes des matrices avec des sous-thèmes et d'améliorer la codification. Nous avons alors pu classer les déterminants internes, psychologiques et externes qui interviennent dans la gestion du risque cyber par le dirigeant de PME.

4. Analyse des résultats

4.1. L'influence du dirigeant de PME dans la gestion du risque cyber dépend de la taille de l'entreprise

Tout d'abord, nos résultats montrent que la gestion du risque cyber est majoritairement assurée par le dirigeant de la PME et cela est d'autant plus le cas lorsque la PME est petite. Elle est parfois assurée par un prestataire externe ou bien un salarié-RSSI. Il est intéressant de constater que pour les plus grandes PME, il existe un service informatique dédié à la gestion de la cybersécurité : « *je n'ai ni les compétences ni le temps pour le faire.* » (Dirigeant n°6). De plus, cela peut également s'expliquer par le fait que plus il y a de salariés dans la PME et plus elle possède des ressources humaines et financières pour assurer la cybersécurité.

Ensuite, l'étude montre que la perception du risque cyber de l'entreprise est particulièrement élevée pour les dirigeants des plus grandes PME : « *Nous collectons des données personnelles, de l'argent donc oui potentiellement nous sommes une cible.* » (Dirigeant n°1) ; « *Je sais que les cyberattaques sont un risque à ne pas négliger.* » (Dirigeant n°6). Ces dirigeants ont tendance à faire confiance aux spécialistes de leur entreprise qui au sein de leurs tâches professionnelles doivent assurer la cybersécurité. A l'inverse, les dirigeants des plus petites PME pensent moins être des cibles attractives pour les pirates informatiques : « *Non pas vraiment, je n'ai pas de données sensibles donc je n'y ai jamais consacré beaucoup de temps.* » (Dirigeant n°2). « *Je suis une toute petite entreprise et n'ai pas beaucoup de clients ni de visibilité.* » (Dirigeant n°4).

Les experts interrogés sont en phase avec l'auto-perception des dirigeants. Ils montrent que ces derniers ont une faible perception du risque cyber pour leur entreprise : « *Dans l'esprit des TPE/PME, leur petite taille et moyens financiers ne sont pas un enjeu pour le monde du piratage informatique* » (Expert n°7). « *la mise en œuvre et la réflexion sur les mesures à apporter sont inexistantes.* » (Expert n°4). Lors d'un entretien, un expert pense que les dirigeants n'ont « *pas toujours la bonne perception du rapport coût/bénéfice de la sécurité, et pensent plus au time to market pour générer rapidement du profit.* ». (Expert n°3). Pourtant, les PME représentent une cible intéressante pour les pirates informatiques, tout comme les grandes entreprises. Les verbatims d'experts le montrent : « *Un grand OUI. [...] ce sont souvent des cibles faciles, car peu au courant des dangers, peu équipés pour lutter et pas souvent conscientes de la menace.* » (Expert n°3) ; « *les PME sont clairement attractives car elles peuvent être un tremplin pour atteindre des ETI* » (Expert n°10).

De plus, le dirigeant n'est pas nécessairement porteur de projet de cybersécurité pour gérer le risque cyber. La majorité des entretiens révèlent que les dirigeants ne disposent que de la protection informatique minimale, c'est-à-dire d'un anti-virus et d'un pare-feu. Les dirigeants perçoivent en général leur niveau de cybersécurité comme basique. Dès lors qu'il le peut, il délègue les missions associées : « *Je délègue car il convient d'avoir des compétences techniques spécifiques.* » (Dirigeant n°1). Néanmoins, pour les dirigeants de PME ne pouvant les déléguer, il s'efforce d'appliquer le minimum de cybersécurité requis (souvent un anti-virus) : « *Non pas spécialement je fais le minimum requis* » ; « *antivirus à jour et de faire des nettoyages* » (Dirigeant n°11).

Les experts sont également unanimes, le niveau de cybersécurité des PME est faible : « *Peu de TPE/PME que j'accompagne ont défini un budget dédié à la sécurité de l'information. Et sans ces budgets il n'y a pas de mesures adéquates, le strict minimum est appliqué et repose sur des outils gratuits et non maîtrisés* » (Expert n°4). « *je rencontre régulièrement des RSSI qui pensent avoir construit un château fort alors qu'il n'y a aucun barreau aux fenêtres* » (Expert n°2) « *Souvent il y a une partie d'évangélisation, il faut expliquer pourquoi ce qu'ils ont mis en place ne va pas et ce qu'il faut mettre en place.* » (Expert n°8). De plus, il semble persister des problématiques liées à une compréhension non optimale des enjeux du risque cyber par les dirigeants : « *il y a une méconnaissance des enjeux de la cybersécurité et de ses conséquences* » (Expert n°6).

Cette première partie des résultats montre que plus la PME est grande et plus le dirigeant aura conscience des enjeux liés au risque cyber. Néanmoins, ce dernier privilégiera la délégation des tâches de cybersécurité aux salariés compétents lorsqu'ils existent. A l'inverse, au sein des plus petites PME, le dirigeant doit souvent assurer seul les tâches liées à la cybersécurité et cela semble parfois compliqué à mettre en œuvre à cause du manque de connaissances. Ainsi, d'une manière générale, nous constatons que le dirigeant veille à appliquer le minimum pour la cybersécurité. Nous pouvons alors constater qu'il existe une conscience du risque cyber mais qui est éloignée des préoccupations quotidiennes.

4.2. Un intérêt renforcé lorsque le dirigeant est proche du risque cyber

Il est également intéressant de constater que l'expérience d'avoir subi une attaque informatique va grandement influencer la perception du dirigeant de PME à l'égard de la gestion du risque cyber : « *Le fait d'avoir été victime d'attaque m'a fait prendre conscience que ce n'est pas un*

sujet à prendre à la légère » (Dirigeant n°12) ; « L'influence est plutôt intrinsèque notamment à cause de mon piratage de mail » (Dirigeant n°2).

L'avis de la majorité des experts converge avec celui des dirigeants car pour eux le plus grand facteur motivationnel à la prise de mesures en faveur de la cybersécurité est le fait de subir une attaque informatique : *« un des leviers les plus marquant pour pousser un dirigeant à prendre des mesures. »* et cela est notamment *« le moyen le plus efficace pour faire changer la perception du dirigeant. »* (Expert n°4). Par ailleurs, à la suite d'une attaque informatique, la façon dont le dirigeant gère le risque cyber change : *« Oui à la suite d'une attaque les budgets alloués à la sécurité se débloquent et l'informatique devient prioritaire pour le dirigeant. »* (Expert n°2). Néanmoins, certains experts montrent que l'intérêt n'est que temporaire : *« d'abord c'est « panique à bord » ensuite dès que les activités auront été rétablies, l'importance de la cybersécurité sera de nouveau revue à la baisse... »* (Expert n°7).

De plus, selon les experts, la gestion du risque cyber par le dirigeant est également très influencée par les attaques que peuvent subir d'autres structures similaires. En effet, c'est le cas pour quasiment tous les experts : *« Une entreprise voisine ou un concurrent frappé par une attaque aura une incidence directe sur les décisions de sécurité informatique »* (Expert n°2) ; *« apprendre qu'une structure proche par exemple en taille et en relation ou géographiquement, a été victime de piratage. »* (Expert n°7). *« au même titre que si son concurrent est victime d'une attaque. »* (Dirigeant n°4).

4.3. Des facteurs économiques, réglementaires et réputationnels de plus en plus marqués

Trois types de facteurs en particulier influencent les dirigeants de PME dans la gestion du risque cyber : les facteurs économiques, réglementaires et réputationnels. Un des déterminants principaux ayant un rôle majeur dans la gestion du risque cyber est le déterminant économique. En effet, les pertes financières et l'arrêt d'activité sont deux conséquences très redoutées par les dirigeants de PME : *« Une attaque nous ferait perdre des semaines de chiffre d'affaires »* (Dirigeant n°7). *« Un blocage du calendrier de réservations serait ennuyeux. »* (Dirigeant n°3).

De plus, la réglementation à respecter et notamment le RGPD est un autre déterminant majeur qui intervient dans la gestion du risque cyber, notamment car le dirigeant est le responsable légal de la PME : *« Ce serait se mettre en conformité avec la réglementation, qui est parfois compliqué à comprendre mais on n'a pas le choix »* (Dirigeant n°8). Les experts mettent également en avant l'importance de la réglementation dans la gestion du risque cyber : *« les dirigeants veulent quand même respecter la loi. »* (Expert n°8). *« exemple typique le RGPD qui a permis de faire prendre conscience aux dirigeants que des risques existent »* (Expert n°4).

Enfin, l'atteinte à la réputation de l'entreprise va également influencer la gestion de la cybersécurité par le PME et encourager le dirigeant à investir dans des outils de protection : *« Une mauvaise réputation ! Mon activité étant basée sur ma notoriété et un réseau ce serait fatal. »* (Dirigeant n°2). *« Il est dur de gagner la confiance des clients mais il est très facile de la perdre. »* (Dirigeant n°4).

4.4. Les facteurs externes à la PME influencent la gestion du risque cyber

L'étude a montré que les dirigeants de PME ne se renseignent ni spontanément ni volontairement sur le sujet de la cybersécurité. En effet, la grande partie des interviewés ont révélés n'avoir aucun mode de renseignement à l'égard de la cybersécurité. Souvent,

l'information vient à eux naturellement principalement par les biais des médias et de l'actualité. Cela converge avec le fait que les dirigeants soient tout de même conscients que le risque cyber existe (mais peu pour leur propre entreprise) : « *me renseigne pas spécialement, j'en entends parler au travers les médias* » (Dirigeant n°9) ; « *Tous les moyens sont bons pour se renseigner mais je ne le fais pas forcément* » (Dirigeant n°12). D'autres entretiens ont montré que l'information sur la cybersécurité était poussée et non tirée d'une démarche de renseignements initiée personnellement. C'est notamment le cas au travers des réseaux sociaux et des syndicats professionnels : « *via notre syndicat professionnel quand ils font passer des informations* » (Dirigeant n°10).

Les médias représentent donc un facteur d'influence majeur pour les dirigeants, mais selon les experts avec un moindre poids qui eux mettent plus en avant les attaques sur structures similaires. Ensuite et selon les experts, d'autres sources d'influences impactent la perception telles que la Réglementation en général qui a un rôle d'influence certain puisqu'obligatoire, le fait de subir une attaque, ou encore le fait de tout simplement ignorer, voire la volonté d'ignorer la SSI. Les dirigeants subissent donc sans doute les facteurs d'influence cités par les experts implicitement, sans en avoir réellement conscience. Les médias qui véhiculent constamment l'information concernant les risques cyber (attaques informatiques, bonnes pratiques à adopter, messages de vigilance, etc) influencent donc la préoccupation et la gestion des risques cyber par les dirigeants de PME.

4.5. Un sentiment de peur et d'incompétence qui conduit à l'évitement

La recherche a étudié les sentiments des dirigeants de PME en tant que déterminant dans la gestion du risque cyber. Il s'avère que face à la cybersécurité, les dirigeants ressentent principalement de l'incompétence et de la peur. « *C'est de l'incompétence et du désintérêt* » (Dirigeant n°3). « *Je ressens de l'incompétence parce que je n'y connais rien.* » (Dirigeant n°2). Les dirigeants ressentent également beaucoup de peur et d'anxiété face à cette problématique : « *Je me sens incompétente car je n'ai pas les connaissances et les compétences suffisantes pour favoriser seule une sécurité au sein de mon activité. De là découle un peu de peur et d'anxiété* » (Dirigeant n°4) ; « *peur de perdre des données, des photos, ou des documents importants* » (Dirigeant n°11).

Les sentiments de peur et d'incompétence ressentis par les dirigeants à l'égard du risque cyber montrent que ces facteurs peuvent exercer une influence négative dans leur prise de mesures en faveur de la cybersécurité. En effet, la mauvaise appréhension du domaine peut les décourager et engendrer un désintéressement les menant à l'évitement de la gestion du risque cyber optimale dans l'entreprise. Il est également intéressant de constater que les experts ont souvent cité la peur comme facteur déterminant dans la gestion du risque cyber par le dirigeant : « *la peur d'être attaqué* » (Expert n°10) « *les attaques sur d'autres entreprises associées à un sentiment de peur* » (Expert n°6). De plus, selon certains experts et en rejoignant l'opinion des dirigeants, les médias ont également une influence sur le déterminant psychologique de la peur du dirigeant : « *les médias ne cessent d'entretenir une peur sur mille sujets* » (Expert n°7).

5. Discussion

5.1 Contributions théoriques

5.1.1 Une perception du risque cyber de plus en plus influencée par des facteurs externes

La littérature montre que les dirigeants de PME ont une faible conscience du risque cyber (Dojkovski *et al.*, 2006 ; Njenga et Jordaan, 2016), et notre étude va aux premiers abords en ce sens car nous constatons que les dirigeants ne pensent pas spécifiquement être une cible attractive pour les pirates informatiques. Pourtant, les experts interrogés rejoignent la littérature en affirmant qu'elles y sont sujettes et que les dirigeants n'ont pas une forte conscience du risque.

Néanmoins, l'étude montre que pour les dirigeants de PME, les médias et l'actualité qui prennent de plus en plus d'ampleur sont des déterminants externes qui influencent leur gestion du risque cyber. En effet, la plupart des dirigeants ont avoué ne pas se renseigner volontairement sur le sujet de la cybersécurité, mais que souvent l'information venait à eux naturellement. Contrairement à ce que véhicule globalement la littérature, notre apport théorique est alors de constater que les dirigeants sont bien conscients du risque cyber d'une manière générale malgré eux, car la société actuelle pousse constamment les informations vers les individus. Néanmoins, ils ne se sentent pas directement concernés par les enjeux de la cybersécurité à titre personnel et pour leur propre entreprise.

De plus, cette recherche confirme et complète les travaux actuels mettant en évidence que le déterminant économique (Strupczewski, 2021 ; Douzet et Héon, 2013), le déterminant réputationnel (Strupczewski, 2021), ainsi que le déterminant réglementaire (Mourrain et Leconte, 2019 ; Barlette, 2012) ont bien une influence dans la gestion du risque cyber en organisation. Néanmoins, l'apport de cette étude est que nous avons directement le point de vue du dirigeant et cela est appliqué au contexte de PME. En effet, l'étude montre que ce sont les impacts sur l'organisation qui découleraient de ces trois déterminants que le dirigeant redouterait de plus à la suite d'une attaque informatique.

5.1.2 Le sentiment de peur : un rôle complexe et paradoxal dans la cybersécurité

L'étude montre que l'incompétence et la peur sont les deux sentiments principaux ressentis par les dirigeants de PME à l'égard de la cybersécurité. Le fait que les dirigeants ressentent des sentiments à tendance péjorative peut être paradoxal avec leur faible conscience du risque cyber pour leur propre entreprise. Pourquoi ressentent-ils de l'incompétence et de la peur si leur conscience du risque cyber envers leur entreprise est faible ?

En se basant sur l'EPPM qui montre qu'à la suite de l'évaluation de la menace perçue les individus préfèrent éviter l'information pour atténuer leur peur au lieu de mettre en place des mesures pour atténuer les menaces (Witte, 1994), nous pouvons supposer que les médias (principal facteur d'influence dans la gestion du risque cyber pour le dirigeant) communiquent de la peur (principal sentiment ressenti par les dirigeants à l'égard de la cybersécurité), ce qui influence négativement les dirigeants dans leur gestion du risque cyber. Les médias conduiraient donc le dirigeant à l'évitement d'une gestion du risque cyber optimale.

Finalement, nous constatons que le dirigeant a justement une forte perception du risque cyber mais que sa peur lui laisse percevoir un manque de contrôle et d'efficacité pour y faire face. Par ailleurs, cela rejoint le travail de Nabi et Myrick (2019) qui montre que le simple fait de penser être incapable de répondre à un risque génère de l'incertitude et un sentiment de peur amplifié.

5.1.3 Un nouveau déterminant de la gestion du risque cyber : la « proximité avec le risque cyber »

Cette recherche nous permet d'apporter un nouveau déterminant à la littérature s'appliquant en particulier aux dirigeants de PME françaises concernant la gestion du risque cyber : la proximité avec le risque. En effet, nous constatons que c'est lorsque le dirigeant est proche du risque, que sa perception et son implication dans la gestion du risque cyber augmentent. Plusieurs facteurs nous permettent d'affirmer cela. Premièrement, nous constatons que le fait de subir une attaque influence positivement le dirigeant à investir dans des outils de cybersécurité. Deuxièmement, les attaques informatiques que peuvent subir d'autres structures similaires est un facteur d'influence majeur dans leur gestion de la cybersécurité. Troisièmement, les dirigeants gérant un nombre d'utilisateurs importants traitant beaucoup de données sont davantage sensibles aux enjeux de la cybersécurité car le risque cyber y est plus important.

Torrès (2003) montre le rôle majeur qu'exerce la proximité dans la gestion des entreprises de petites tailles en se basant sur l'effet de grossissement. Notre étude va en ce sens puisqu'elle montre que les PME sont grandement influencées par la proximité dans leur gestion du risque cyber. Par ailleurs, en ouverture de fin d'article, Torrès (2003) se demande sous quelle condition la proximité est un vecteur d'efficacité pour la petite entreprise. Dans un contexte de gestion du risque cyber, notre étude nous permet de voir que la proximité avec le risque cyber va être un facteur déclencheur d'action en faveur de la cybersécurité. Nous pouvons alors définir la « proximité avec le risque cyber » comme une situation où un facteur déclencheur va impacter positivement la conscience du risque cyber par la personne en charge de la cybersécurité et favoriser l'implication dans la SSI.

5.2 Contributions managériales

Sur un plan managérial, la recherche permet de comprendre les déterminants qui interviennent dans la gestion du risque cyber par les dirigeants de PME. En particulier, l'étude montre que la cible de l'étude n'a pas réellement une faible perception du risque cyber comme cela est en général véhiculé dans la littérature (Dojkovski *et al.*, 2006 ; Njenga et Jordaan, 2016), au contraire, les dirigeants de PME en ont une forte conscience. En effet, le sujet du risque cyber devient de nos jours omniprésents au sein des médias et être informé et un minimum sensibilisé devient une évidence. Pourtant, il existe un certain évitement de l'information par les dirigeants, notamment dû à un sentiment de peur et de manque de compétences certain en gestion du risque cyber.

Au sein de leur rôle de leader et d'influenceur sur les employés dans la gestion du risque cyber (Barlette *et al.*, 2017 ; Barton *et al.*, 2016 ; Thong, 1999), cette étude permet aux dirigeants de prendre conscience de l'importance de leur l'implication. La perception des experts du secteur de la cybersécurité confrontée à celle des dirigeants permet notamment d'obtenir une vision globale concernant les PME, qui à l'avenir peut permettre aux dirigeants de se remettre en question. Dans tous les cas, les apports managériaux sont destinés aux deux parties : les dirigeants de PME et les entreprises du marché de la cybersécurité. En effet, pour les dirigeants les recommandations représentent des mesures à mettre en place, mais la plupart ne sont pas envisageables sans la participation dans l'action d'un expert de la cybersécurité.

6. Conclusion

Cette étude avait pour objectif d'apporter un éclairage concernant les déterminants qui interviennent dans la gestion du risque cyber par le dirigeant de PME. Nous avons identifié trois grandes catégories de déterminants : internes, psychologiques et externes.

La recherche corrobore certains déterminants présents dans la littérature comme la place centrale du dirigeant dans la gestion de la cybersécurité, son faible niveau de compétences en la matière, l'influence de la taille de la PME dans la gestion du risque cyber, ou encore l'importance des déterminants économiques, réputationnels et règlementaires.

Les résultats mettent également en lumière deux autres facteurs qui n'ont pas été étudiés dans la littérature sur la cybersécurité en PME. Premièrement, la recherche met en exergue le sentiment de peur que peut ressentir le dirigeant de PME face au risque cyber qui pourrait être relié à l'influence que les médias ont sur lui. Cela nous permet de dire que le dirigeant de PME a une conscience du risque cyber bien présente mais que la peur et l'incompréhension face au sujet l'empêchent de mettre en place une gestion du risque cyber optimale. En effet, comme expliqué dans l'EPPM (1994), lorsque l'individu perçoit une menace sur laquelle il pense ne pas être capable d'agir, il préférera éviter l'information pour atténuer sa peur au lieu de mettre en place des mesures pour atténuer la menace. Deuxièmement, la recherche met en lumière l'existence d'un facteur que nous avons appelé « proximité avec le risque cyber ». En effet, plus le dirigeant se trouve dans une situation de proximité avec le risque, plus ce dernier est perçu. In fine, nous proposons une définition de la « proximité avec le risque cyber ». Les résultats de cette recherche permettent ainsi d'enrichir la littérature sur la gestion du risque cyber,

De par son caractère exploratoire, la principale limite de cette étude est liée à l'hétérogénéité des profils des interviewés et au nombre restreint de dirigeants de PME interrogés. De futures recherches pourraient se centrer sur les dirigeants notamment de PME présentant un plus grand nombre d'utilisateurs informatiques.

Les recherches futures auraient notamment bénéfice à porter attention au sentiment de peur communiqué par les médias et leur impact sur l'agilité de la PME dans la gestion du risque cyber. La compréhension d'une meilleure sécurisation de la cybersécurité est un enjeu majeur dans un contexte de double augmentation de l'usage du numérique et du nombre d'attaques informatiques ciblant les entreprises.

6. Bibliographie

Abaaoukide, K. et Bentaleb, C. (2011). La gestion de l'urgence dans les PME au Maroc : Perceptions et pratiques de gestion. *Revue Management & Avenir*, 3(43), 143-163.

Agence Nationale de la Sécurité du Système d'Information (2022). Panorama de la menace informatique 2021. Rapport n° CERTFR-2022-CTI-002, Paris, France.

Agence Nationale de la Sécurité du Système d'Information (2022). *Glossaire - Document en ligne*. Récupéré le 03 mars 2022 du site de l'auteur : <https://www.ssi.gouv.fr/entreprise/glossaire/c/>.

Alahmari, A. et Duncan, B. (2020). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. Dans *IEEE, 2020 international conference on cyber situational awareness, data analytics and assessment (CyberSA)* (p. 1-5). Piscataway, Etats-Unis.

Ashenden, D. (2008). Information Security Management: A Human Challenge ?. *Information Security Technical Report*, 13(4), 195-201.

Bada, M., Sasse, A.M. et Nurse, J.R. (2015). Cyber security awareness campaigns: Why do they fail to change behaviour ?. Dans *International Conference on Cyber Security for Sustainable Society* (p. 118-131). Coventry, Royaume-Unis.

Barlette, Y. (2012). Implication et action des dirigeants : quelles pistes pour améliorer la sécurité de l'information en PME ?. *Systèmes d'information & management*, 17(2), 115-149.

- Barlette, Y., Gundolf, K. et Jaouen, A. (2017). CEOs' information security behavior in SMEs: Does ownership matter ?. *Systèmes d'Information et Management*, 22(3), 7-45.
- Barton, K.A., Tejay, G., Lane, M. et Terrell, S. (2016). Information System Security Commitment: A Study of External Influences on Senior Management. *Computers & Security*, 59, 9-25.
- Birley, S. (1982). Corporate strategy and the small firm. *Journal of General Management*, 8(2), 82-86.
- Boss, S.R., Kirsch, L.J., Angermeier, I., Shingler, R.A. et Boss, R.W. (2009). If Someone is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security. *European Journal of Information Systems*, 18(2), 151-164.
- Boss, S.R., Galletta D.F., Lowry P.B., Moody G.D. et Polak P. (2015). What do Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors. *MIS Quarterly*, 39(3), 837-864.
- Chatterjee, D. (2019). Should executives go to jail over cyber attacks ?. *Journal of Organizational Computing & Electronic Commerce*, 29(1), 1-3.
- Claveau, N., Perez, M. et Serboff, T. (2018). Myopie et risque de défaillance en PME. *Revue internationale P.M.E.*, 31(3-4), 95-130.
- Cook, T.D. et Campbell, D.T. (1979). *Quasi-experimentation: Design and analysis issues for field settings*. Chicago, Rand McNally.
- Cragg, P., Caldeira, M. et Ward, J. (2011). Organizational Information Systems Competences in Small and Medium-Sized Enterprises. *Information & Management*, 48(8), 353-363.
- Dojkovski, S., Lichtenstein, S. et Warren, M. (2006). Challenges in fostering an information security culture in Australian small and medium sized enterprises. Dans Academic Conferences Limited, *ECIW2006: proceedings of the 5th European conference on Information Warfare and Security* (p. 31-40). Kidmore End, Angleterre.
- Douzet, F. et Héon, S. (2013). L'analyse du risque cyber, emblématique d'un dialogue nécessaire. *Sécurité et stratégie*, 14(3), 44-52.
- Dutta, A. et McCrohan, K. (2002). Management's role in information security in cyber economy. *California Management Review*, 45(1), 67-87.
- Evrard, Y., Pras B. et Roux, E. (2003). *Market- Etudes et recherches en marketing*, 3ème Edition. Paris, Dunod.
- Fortin, M.-F. et Gagnon, J. (2016). *Fondements et étapes du processus de recherche. Méthodes quantitatives et qualitatives* (3ème édition). Montréal, Chenelière Education.
- Germain, E. (2021). Le numérique vu au travers de sa sécurité : le prisme de l'ANSSI. *Revue Défense Nationale*, 837(2), 84-88.
- Goodhue, D. L. et Straub, D.W. (1991). Security concerns of systems users: a study of perceptions of the adequacy of security measures. *Information and Management*, 20(1), 13-27.
- Gupta, A. et Hammond, R. (2005). Information systems security issues and decisions for small businesses: an empirical examination. *Information Management and Computer Security*, 13(4), 297-310.
- Heidt, M., Gerlach, J.P. et Buxmann, P. (2019). Investigating the security divide between SME and large companies: How SME characteristics influence organizational IT security investments. *Information Systems Frontiers*, 21(6), 1285-1305.
- Howard, L.S. (2018, 05 mars). *SMEs underestimate cyber risks which could prove 'fatal': Allianz report - Document en ligne*. Récupéré le 27 septembre 2021 du site de l'auteur : <https://www.insurancejournal.com/magazines/mag-features/2018/03/05/481912.htm>
- Institut National de la Statistique et des Etudes Economiques (2021). *Caractéristiques des entreprises par catégorie - Document en ligne*. Récupéré le 28 août 2021 du site de l'auteur : [Caractéristiques des entreprises par catégorie | Insee](#).

- Johnston, A.C. et Hale, R. (2009). Improved Security through Information Security Governance. *Communications of the ACM*, 52(1), 126-129.
- Johnson, A.M. (2009). Business and security executives views of information security investment drivers: Results from a delphi study. *Journal of Information Privacy and Security*, 5(1), 3-27.
- St-Pierre, J., Therrien, C. (2007). L'évaluation du risque des PME : l'objectivité totale est-elle possible ?. *Xes Journées scientifiques du Réseau Entrepreneuriat de l'AUF*. Antananarive, Madagascar.
- Julien, P.-A. (1990). Vers une Typologie Multicritère des PME. *Revue Internationale PME*, 3(3-4), 411-425.
- Kouabenan, D., Cadet, B., Hermand, D. et Munoz Sastre, M.T. (2006). *Psychologie du risque : identifier, évaluer, prévenir*. Bruxelles, De Boeck.
- Kotulic, A.G. et Clark, J.G. (2004). Why There Aren't More Information Security Research Studies. *Information & Management*, 41(5), 597-607.
- Lee, Y. et Larsen, K.R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, 18(2), 177-187.
- Miles, M.B., Huberman, A.M. et Saldana, J. (2018). *Qualitative data analysis: A methods sourcebook*. Washington, Sage Publications.
- Mintzberg, H. (1989). The Structuring of Organizations. Dans *Readings in Strategic Management* (p. 322-352). Londres, Angleterre.
- Mourrain A. et Leconte P. (2019). Comment la démarche projet de développement d'un Système d'information est-elle impactée par le RGPD ? Cas d'une ETI du secteur de l'assurance. *24ème colloque de l'Association information et Management*. Nantes, France.
- Nabi, R.L. et Myrick, J.G. (2019). Appels à la peur édifians : Considérer le rôle de l'espoir dans les messages persuasifs basés sur la peur. *Communication sur la santé*. 34(4), 463-474.
- Njenga, K. et Jordaan, P. (2016). We Want to Do It Our Way: The Neutralisation Approach to Managing Information Systems Security by Small Businesses. *African Journal of Information Systems*, 8(1), 42-63.
- Oppens, (2020, 04 mars). *Faillites de PME après une cyberattaque : ce n'est pas une légende – Document en ligne*. Récupéré le 22 septembre 2021 du site de l'auteur : <https://www.oppens.fr/faillite-pme-cyberattaque-lise-charmel/>.
- Pellegrin-Boucher, E., Le Roy, F. et Gurău', C. (2018). Managing selling coopetition: a case study of the ERP industry. *European Management Review*, 15(1), 37-56.
- Prnewswire, (2015, 05 octobre). *Small and Midsize Businesses Learn to Protect Their Digital Assets During National Cyber Security Awareness Month - Document en ligne*. Récupéré le 25 mai 2022 du site de l'auteur : <https://www.prnewswire.com/news-releases/small-and-midsize-businesses-learn-to-protect-their-digital-assets-during-national-cyber-security-awareness-month-300154074.html>
- Rainer, R. K., Marshall, T. E., Knapp, K. J. et Montgomery, G. H. (2007). Do Information Security Professionals and Business Managers View Information Security Issues Differently ?. *Information Systems Security*, 16(2), 100-108.
- Van Schaik, P., Jansen, J., Onibokun, J., Camp, J. et Kusev, P. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behaviour. *Computers in Human Behavior*, 78, 283-297.
- Van Schaik, P., Renaud, K., Wilson, C., Jansen, J. et Onibokun, J. (2020). Risk as affect: The affect heuristic in cybersecurity. *Computers & Security*, 90, 101651.
- Ventre, D. (2016). De l'utilité des indices de cybersécurité. *Sécurité et Stratégie*, 2(22), 5-11.
- Sirur, S., Nurse, J. R. et Webb, H. (2018). Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR). Dans *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security* (p. 88-95). Toronto, Canada.

Stasiak, K. (2018, 26 juillet). *Middle-market companies underestimate cybersecurity risks* - Document en ligne.. Récupéré le 15 octobre 2021 du site de l'auteur : <https://www.industryweek.com/leadership/article/22026028/middlemarket-companies-underestimate-cybersecurity-risks>.

Straub, D. W. et Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS quarterly*, 441-469.

Taylor, A. (2005). An operations perspective on strategic alliance success factors. *International Journal of Operations & Production Management*, 25(5), 469-490.

Taylor, R.G. et Brice, J. (2012). Fact or Fiction? A Study of Managerial Perceptions Applied to an Analysis of Organizational Security Risk. *Journal of Organizational Culture, Communications and Conflict*, 16(1), 1-23.

Thong, J.Y.L. (1999). An integrated model of information systems adoption in small businesses. *Journal of Management Information Systems*, 15(4), 187-214.

Torrès, O. (2003). Petitesse des entreprises et grossissement des effets de proximité. *Revue française de gestion*, 3(144), 119-138.

Strupczewski, G. (2021). Defining cyber risk, *Safety Sciences*, 135, 1-10.

Wartick, S-L. et Cochran P-L. (1985). The evolution of the corporate social performance model. *Academy of Management Review*, 10(4), 758-769.

Witte, K. (1992). Remettre la peur dans les appels à la peur : le modèle de processus parallèle étendu. *Communications Monographies*. 59(4), 329-349.

Witte, K. (1994). Contrôle de la peur et contrôle du danger : un test du modèle de processus parallèle étendu (EPPM). *Communications Monographies*, 61(2), 113-134.

Williams, P. (2007). Executive and Board Roles in Information Security. *Network Security*, 2007(8), 11-14.

Yin, R.K. (2015). *Qualitative research from start to finish*. New York, Guilford Publications.

Zacca, R., Dayan, M. et Elbanna, S. (2017). The influence of conflict and intuition on explorative new products and performance in SMEs. *Journal of Small Business and Enterprise Development*, 24(4), 950-970.

Zadeh, A.H., Jeyaraj, A., Biros, D., (2020). Characterizing Cybersecurity Threats to Organizations in Support of Risk Mitigation Decisions. *e-Service Journal*, 12(2), 1-34.

Zwikael, O. (2008). Top management involvement in project management: A cross country study of the software industry. *International Journal of Managing Projects in Business*, 1(4), 498-511.