# Les comportements des acteurs en matière de sécurité de l'information et leurs déterminants : les théories du 'coping' et leur enrichissement

Yves Barlette

▶ **To cite this version:**

Yves Barlette. Les comportements des acteurs en matière de sécurité de l'information et leurs déterminants : les théories du 'coping' et leur enrichissement. Gestion et management. Université de Montpellier, 2020. tel-03037272

**HAL Id: tel-03037272**
**https://hal.science/tel-03037272**

Submitted on 3 Dec 2020

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

**Université de Montpellier**

EDEG

**Mémoire en vue de l'obtention d'une**

**Habilitation à Diriger des Recherches**

en Sciences de Gestion

Section CNU 06

**Version compacte**

# Les comportements des acteurs en matière de sécurité de l'information et leurs déterminants
# Les théories du 'coping' et leur enrichissement

*Présenté par Yves BARLETTE*

**Soutenue le 24 septembre 2020**

Devant le jury composé de :


Pr Alain Cucchi, Université de la Réunion, Saint-Denis, France
alain.cucchi@univ-reunion.fr

Pr Christophe Elie-Dit-Cosaque, Université Paris-Dauphine, France
christophe.elie-dit-cosaque@dauphine.psl.eu

Pr Jean-Fabrice Lebraty, IAE de Lyon, France
jean-fabrice.lebraty@univ-lyon3.fr

Pr Régis Meissonier, IAE de Montpellier, France (Coordinateur)
regis.meissonier@umontpellier.fr

Pr Alain Pinsonneault, Université McGill, Canada
alain.pinsonneault@mcgill.ca

# Sommaire

# Introduction

Si, dans les années 1990, j'avais manifesté un intérêt pour la sécurité de l'information dans un contexte pédagogique, c'est en 2000 que l'IR2I (institut de recherche en intelligence informationnelle) m'a proposé de m'impliquer dans ce domaine en tant que chercheur.

Cette équipe se consacrait surtout à l'intelligence économique, c'est à dire la 'captation' des informations, et à ses dérives, i.e., l'espionnage industriel. Si ces thématiques étaient intéressantes, j'ai été plus attiré par l'autre face de ces problématiques, c'est-à-dire la protection des informations. Ceci m'a amené à étudier, dans un premier temps, la sécurité de l'information (SSI) sur un plan principalement technique et normatif et, après une année de participation dans l'IR2I, j'ai entamé une thèse en septembre 2001, dont l'objectif initial était d'établir une typologie de risques selon les types d'entreprises. Mais très rapidement, l'intuition que la sécurité de l'information était surtout une affaire de comportements s'est imposée à moi. Dès 2002[1], je présentais une communication qui affirmait « *que la sécurité de l'information ne devait pas être uniquement vue comme un problème technique* » et je proposais déjà de « *mieux comprendre les pratiques sécuritaires et de vérifier l'importance de la sensibilisation* » des acteurs en PME. Ma thèse s'est peu à peu orientée vers les comportements relatifs à la sécurité de l'information et leurs déterminants, ces problématiques sont encore à ce jour au cœur de mes centres d'intérêts.

Cette HDR a pour but de mettre en exergue la trajectoire académique donnant du sens aux treize années qui ont suivi l'obtention de ma thèse en décembre 2006, au travers des principaux travaux présentés lors de conférences, des 2 articles actuellement en cours de révision mais surtout des 10 articles publiés dans des revues classées FNEGE/CNRS (cf. C.V. détaillé p.96).

Depuis le début et encore à ce jour, ma principale préoccupation est d'identifier les facteurs qui influencent les comportements des acteurs en termes de sécurité de l'information, que ce soit le comportement des dirigeants, principalement en PME, ou encore celui des salariés.

Les travaux académiques sur ces thèmes ont principalement porté sur les individus, dans un environnement personnel ou professionnel, dans le cadre de leur intention de mettre en place et d'appliquer des mesures de sécurité. Toutefois, ces travaux se sont souvent focalisés sur le respect des règles en place, c'est-à-dire la 'compliance' (Moody *et al.*, 2018), en intégrant des théories basées sur la sanction en cas de non-respect des règles, telles que la théorie de la dissuasion ou 'deterrence theory' (Nance et Straub, 1988 ; Moody *et al.*, 2018). Même si certaines recherches se sont intéressées aux comportements émergeant dans des environnements moins contraints, peu de travaux ont porté sur les dirigeants, notamment en PME (SIM, 2019)[2].

Pourtant, le rôle des dirigeants et décideurs en entreprise en matière de sécurité de l'information, est majeur (Friend et Pagliari, 2000 ; Hu *et al.*, 2012), et ce tout particulièrement dans les PME, car même lorsqu'un département informatique existe, il est rare d'y trouver un responsable sécurité informatique (Pritchard, 2010) comme dans les grandes structures. De plus, même si un dirigeant peut compter sur un professionnel (RSSI, DSI, ou un technicien interne ou externe), la sécurité de l'information n'aura que rarement la priorité sur des

[1] « La sécurité des informations, un facteur de confiance : comment sensibiliser les entreprises ? », colloque « la confiance en management, la gestion du changement et le temps en gestion », 3 octobre 2002, ESC Amiens.

[2] NB : Afin de séparer mes articles et communications des autres références bibliographiques, les citations de mes travaux dans le texte sont sous la forme (SIM, 2008) pour les travaux publiés, ou (IJIM, R3) pour les articles en cours de révision, avec R3 pour 'round 3'. Les références complètes peuvent être retrouvées dans le C.V. détaillé qui se trouve en pages 96 à 103.

nécessités d'évolution ou d'alignement du système d'information, sans compter les problèmes de gestion au jour le jour de l'informatique (Gupta et Hammond, 2005 ; SIM, 2012). En PME, le dirigeant n'aura généralement accès qu'à temps partiel aux services d'un professionnel (SIM, 2012), avec une part très faible du budget informatique accordée à la sécurité de l'information (Clusif, 2018). Pourtant, les travaux sur le TMS ou Top Management Support (Boonstra, 2013 ; Jarvenpaa et Ives, 1991 ; SIM, 2012) ont montré que les dirigeants ont une influence majeure sur la validation de certains projets, sur les budgets affectés à ceux-ci, sur la communication après des employés, voire tout simplement sur les comportements des salariés, du fait de leur autorité ou de leur charisme.

Pour articuler une méta-conception qui permette d'encadrer l'étude des comportements des acteurs relatifs à la SSI et des facteurs qui influent sur ces comportements, plusieurs prismes théoriques pouvaient être envisagés, tels que la théorie institutionnelle ou isomorphique (DiMaggio et Powell, 1983 ; Meyer et Rowan, 1977) qui a été adaptée aux usages et aux comportements en SI et SSI (Angst *et al.*, 2017 ; Cavusoglu *et al.*, 2015 ; Hu *et al.*, 2007), les théories relatives à l'acceptation et à l'adoption des technologies de l'information (Fishbein et Ajzen, 1975 ; Davis *et al.* 1989 ; Venkatesh *et al.*, 2003) et les théories basées sur le 'coping' (Lazarus, 1966, 1991 ; Rogers, 1983 ; Beaudry et Pinsonneault, 2005). Je vais maintenant expliquer pourquoi j'ai choisi le 'coping' comme prisme théorique.

Avant la soutenance de ma thèse en 2006, les approches qui existaient en sécurité de l'information étaient principalement basées sur les théories de l'acceptation des technologies. Mon travail doctoral, même s'il correspondait à une démarche qualitative, a été influencé par des approches plus quantitatives, et a permis de dégager les éléments qui influençaient le plus, et ceux qui au contraire, avaient un effet plus modéré, voire quasi nul sur les comportements des acteurs. Entretemps, des modèles issus de la psychologie clinique sont apparus, basés sur les *théories du coping*, autrement dit 'faire avec' ou 'gérer' (Lazarus, 1966), tels que notamment la théorie de la motivation à la protection (PMT) ou *protection motivation theory* (Rogers, 1983), qui a été adaptée au contexte de la sécurité de l'information (Workman et Gathegi, 2005 ; Workman *et al.*, 2008). Ces modèles s'avérant prometteurs et en phase avec les éléments identifiés dans ma thèse, j'ai opté pour des approches quantitatives pour en tester plusieurs intégrant la PMT. Je les ai appliqués à ma cible initiale, c'est-à-dire les dirigeants et employés de PME.

Dès 2012, j'ai commencé à m'intéresser aux risques en matière de sécurité de l'information relatifs aux technologies dites digitales, en plein développement (Karimi et Walter, 2015 ; Sivarajah *et al.*, 2017). Le 'digital' fait référence aux média sociaux, à l'internet des objets, à la mobilité, et à l'informatique en nuage (ou cloud computing) qui rend accessibles de nombreuses applications et offre de grandes capacités de stockage des informations, et ce à coût réduit (Sultan, 2013) par rapport aux coûts d'acquisition et de maintenance d'un serveur et des applications associées. Ces technologies génèrent des masses énormes d'informations qui constituent le big data, et la littérature académique a montré qu'il s'avère nécessaire, ne serait-ce que pour des aspects stratégiques et de compétitivité, d'extraire de la valeur de ces 'données massives' (Shan *et al.*, 2016). Ces technologies sont dites 'disruptives' (Karimi et Walter, 2015), c'est-à-dire qu'elles offrent la possibilité d'introduire des innovations radicales, mais aussi des changements radicaux et donc des risques majeurs (Venkatraman, 1991). Dans ce contexte, nous avons étudié avec Paméla Baillette[3] le phénomène du BYOD qui facilite la mobilité en entreprise et représente un phénomène original d'adoption inversée des

[3] Paméla Baillette est maître de conférences à l'IAE de Bordeaux et chercheur à l'IRGO depuis fin 2018. Nous avons démarré notre collaboration en juin 2016, alors qu'elle était à l'université de Perpignan (UPVD).

technologies (Leclercq-Vandelannoitte, 2015a, 2015b ; IJIM, 2018) et qui présente à la fois des opportunités mais aussi des dangers importants (IJIM, 2018).

Toujours dans le cadre théorique du coping, le *coping model of user adaptation* (CMUA) a été créé en 2005 par Anne Beaudry et Alain Pinsonneault (2005 ; 2010) afin de prendre en compte les opportunités et les risques associés à l'introduction d'une technologie disruptive en entreprise. Nous avons adopté ce modèle pour étudier dans le contexte du BYOD les opportunités perçues par les dirigeants et par les salariés, mais aussi les risques perçus par ces acteurs en termes de sécurité de l'information (JGIM, 2020 ; IJIM, R3). La PMT et le CMUA étant conceptuellement issus de la théorie du 'coping' (Lazarus, 1966), les théories basées sur le coping se sont naturellement imposées comme le cadre fédérateur de mes travaux (voir figure 1 ci-après).

Ce mémoire est structuré en deux principaux chapitres. Le premier correspond à mon prisme conceptuel fédérateur : le coping. Ce chapitre est subdivisé de la manière suivante : La première partie met l'accent sur les travaux issus de ma thèse. Afin de dépasser les limitations des théories classiques sur l'adoption des technologies pour la compréhension des comportements relatifs à la sécurité, dans une seconde partie j'examinerai la PMT et je présenterai les travaux issus de l'utilisation de ce modèle. Puis, dans une troisième partie, j'examinerai au travers du CMUA les opportunités et dangers relatifs à la mise en place du BYOD en entreprise et je résumerai les travaux qui en ont découlé.

Le chapitre 2 est consacré à l'enrichissement des modèles utilisés, il comporte deux parties. La première partie a pour but de faire le point sur les enrichissements potentiels des modèles du coping, que ce soit en amont (variables indépendantes) ou en aval (variables dépendantes). Afin d'améliorer leur pouvoir prédictif, je rebouclerai dans un premier temps sur les théories classiques de l'adoption des S.I., puis j'examinerai d'autres théories susceptibles d'être complémentaires des modèles du coping, ce qui me permettra de présenter de nouvelles pistes de travaux. La seconde partie ouvre mes travaux à d'autres thèmes, sur lesquels j'ai travaillé ces dernières années en parallèle de mes travaux sur la sécurité des informations, qui constitueront des pistes pour de futures recherches ou de nouveaux encadrements de doctorants.

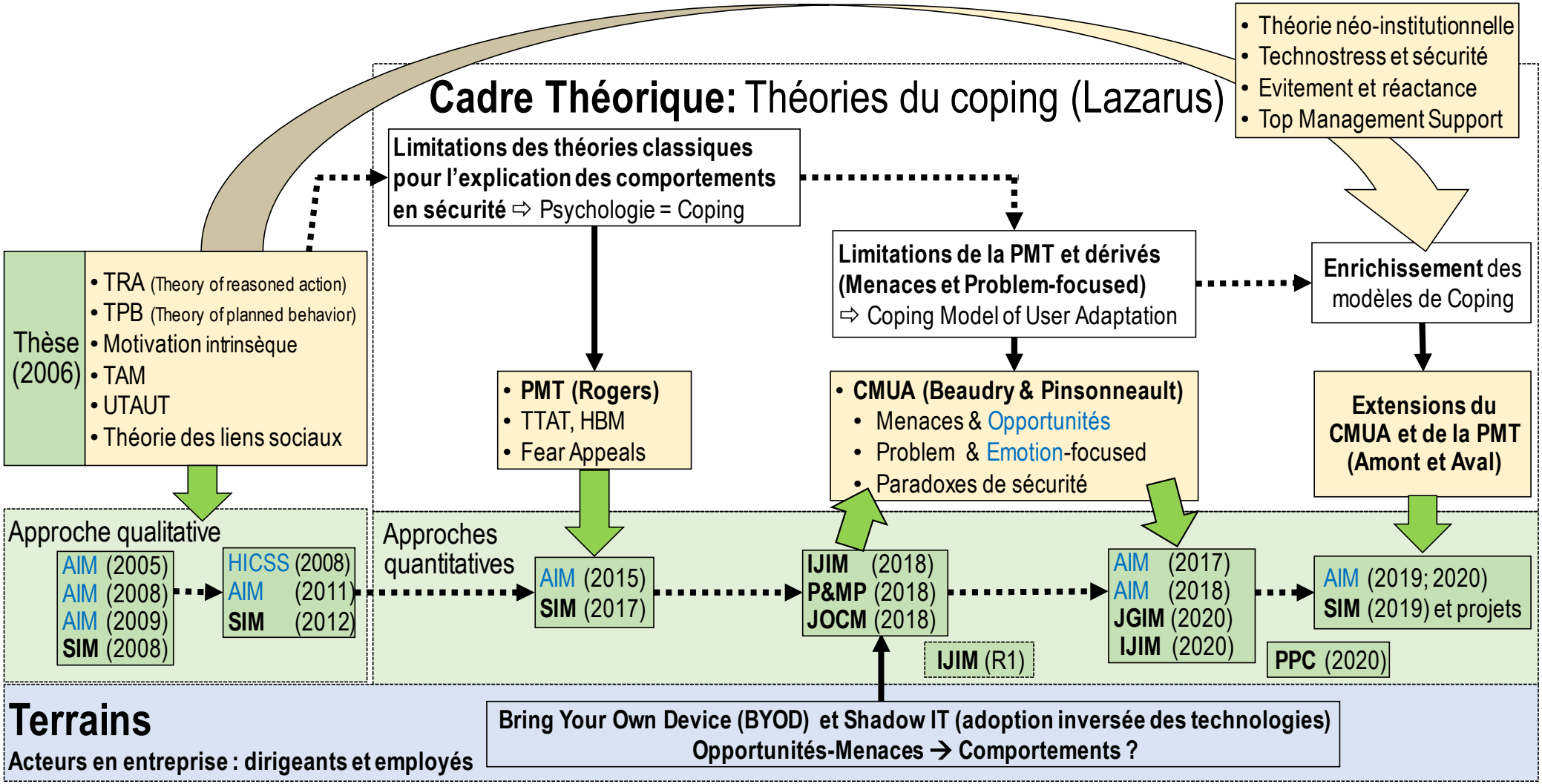


**Figure 1. Cadre théorique fédérateur et contributions résultantes**

**Légende :**

- Fond **Orange** : théories. **Violet** : objets de recherche. **Vert** : production scientifique (pointillés : articles en cours de révision et 'tour' entre parenthèses).
- Texte **Noir** : revues. **Bleu** : conférences.

# 1. Le prisme fédérateur : les théories du Coping

## 1.1. Des premières théories utilisées aux théories du Coping

Mon travail de thèse a consisté en l'exploration des problématiques qui se posaient en matière de comportements relatifs à la sécurité de l'information. Pour cela, et pour chaque type d'acteurs (dirigeant, salariés et techniciens le cas échéant) il s'agissait d'identifier les comportements, la répartition des rôles, et les facteurs qui pouvaient favoriser ou freiner ces comportements. Dans l'optique de mieux comprendre des comportements relatifs à ls SSI, j'ai adopté un positionnement interprétativiste. J'ai utilisé une méthodologie qualitative basée sur des entretiens semi-directifs (Thèse, 2006). Toutefois, pour ne pas partir d'une feuille vierge, j'ai enrichi mon guide d'entretien en tenant compte des théories disponibles à l'époque où a été conduite la partie empirique de ma thèse (2001-2005). A cette époque, je n'avais identifié qu'une seule théorie portant spécifiquement sur le domaine de la sécurité de l'information, c'est-à-dire la *théorie générale de la dissuasion* (Nance et Straub, 1988). J'ai donc ouvert mon cadre théorique à d'autres théories tirées de la criminologie, comme la *théorie des liens sociaux* (Hirschi, 1969), et à celles portant sur *l'acceptation des technologies,* comme l'UTAUT (Venkatesh *et al.*, 2003) qui venait d'être publiée. Le deuxième objectif de l'inclusion de ces théories était de valider leur pertinence pour l'explication des comportements relatifs à la sécurité de l'information. Cette validation sera discutée dans le 1.1.2 et les travaux découlant de la thèse seront présentés dans le 1.1.3.

### *1.1.1. Théories mobilisées dans la thèse*

Ces théories sont regroupées dans les tableaux 1 et 2. Les définitions des construits centraux de ces théories et modèles figurent en annexe 1. Le tableau 1 ci-dessous reprend les théories de l'acceptation des technologies.

| **Théorie de l'action raisonnée** (TRA)<br>Theory of reasoned action | Construits centraux | Variable expliquée |
|---|---|---|
| Cette théorie (Fishbein et Ajzen, 1975 ; Davis *et al.* 1989), tirée de la psychologie sociale, est l'une des plus répandues pour expliquer le comportement humain. | Attitude<br>Normes subjectives | Intention d'utilisation |
| **Théorie du comportement planifié** (TPB)<br>Theory of planned behavior | | |
| Extension de la TRA par Ajzen (1991). | Attitude<br>Normes subjectives<br>Maîtrise perçue | Intention d'utilisation |
| **Modèle d'acceptation de la technologie** (TAM)<br>Technology acceptance model | | |
| Créé par (Davis, 1986, 1989 ; Davis *et al.*, 1989) et adapté au contexte des S.I. pour prédire l'acceptation et l'utilisation des T.I. | Utilité perçue<br>Facilité d'utilisation perçue | Intention d'utilisation |
| **TAM-2** | | |
| Créé par (Venkatesh et Davis, 2000) pour s'adapter au contexte de comportements obligatoires. | Utilité perçue<br>Facilité d'utilisation perçue<br>Normes subjectives | Intention d'utilisation |
| **Théorie unifiée de l'acceptation des technologies** (UTAUT)<br>Unified theory of acceptance and use of technology | | |
| Cette théorie (Venkatesh *et al.*, 2003) reprend une majorité des construits des modèles précédents ainsi que les conditions facilitatrices, tirées du MPCU (Thompson *et al.*, 1991). | Performance espérée<br>Effort attendu<br>Influence sociale<br>Conditions facilitatrices | Intention d'utilisation et utilisation (acceptation) |

**Tableau 1. Théories de l'acceptation des technologies**

Le tableau 2 ci-dessous reprend trois autres théories que j'ai mobilisées dans ma thèse, ainsi que les articles SIM de 2008 et 2012.

| **Théorie des liens sociaux** (SBT)<br>Social bond theory | Construits centraux | Variable expliquée |
|---|---|---|
| Cette théorie (Hirschi, 1969 ; Gottfredson et Hirschi, 1990 ; Jenkins, 1997) est l'une des plus citées en criminologie. Elle postule qu'une personne devient délinquante quand ses liens sociaux sont faibles ou inexistants. | Attachement, Devoir, Implication, Croyances, Apprentissage par observation Identification aux autres | Intention |
| **Modèle de la motivation** (MM) | | |
| Ce modèle (Deci, 1975 ; Deci et Ryan, 1985 ; Davis *et al.*, 1992 ; Vallerand, 1997) est tiré de la psychologie. Il explique certains comportements dans le domaine des S.I., notamment l'adoption et l'utilisation des T.I. (Davis *et al.*, 1992 ; Venkatesh et Speier, 1999). | Motivation intrinsèque<br>Motivation extrinsèque | Intention |
| **Théorie générale de la dissuasion** (GDT)<br>General deterrence theory | | |
| Cette théorie (Nance et Straub, 1988) postule qu'un individu ayant l'intention de commettre des actes répréhensibles en sera dissuadé s'il est convaincu que la probabilité d'être pris et sévèrement puni est quasi certaine (Straub et Welke, 1998). | Sévérité de la punition<br>Certitude d'être détecté | Intention de se conformer aux règles |

**Tableau 2. Théories des liens sociaux, de la motivation intrinsèque et de la dissuasion**

### *1.1.2. Discussion de l'applicabilité des théories mobilisées aux comportements en SSI*

Après la conduite des entretiens semi-directifs et une analyse des discours, il est ressorti de mes résultats que certains construits théoriques semblaient avoir un impact bien plus important que d'autres sur les comportements relatifs à la sécurité de l'information. Dans le tableau 3 ci-dessous, on retrouve notamment la motivation intrinsèque et la théorie des liens sociaux. Même si les normes subjectives ressortent, très peu des construits tirés des théories de l'acceptation des technologies sont pertinents dans le contexte de la SSI, reflétant le fait que l'on ne peut, de manière simple, assimiler une action relative à la sécurité à une utilisation ou une implémentation de moyens technologiques, matériels ou logiciels. En effet, la notion de risque apparait comme plus virtuelle, du fait d'une probabilité qui, à court terme en tout cas, peut sembler faible, voire négligeable. De la même manière, la performance espérée ou l'utilité perçue d'une mesure ou d'un comportement relatif à la sécurité est moins apparente que celle relative à l'adoption d'un logiciel d'entreprise.

| Eléments ressortant des entretiens | | Variables, construits ou concepts | Modèle ou théorie |
|---|---|---|---|
| **Motivations** | | **Construits** | |
| **Eléments majeurs de motivation** | Personnel: motivation, conviction, valeur, viscéral | Motivation intrinsèque | Modèle de la motivation |
| | Poste, fonction, responsabilité | Devoir | Théorie des liens sociaux |
| | Préservation de mon 'intimité', Ils n'ont pas à savoir | Motivation intrinsèque / Privacy concern | Modèle motivation / Privacy |
| | Pour/Loyauté à /Pérennité de l'entreprise | Attachement | Théorie des liens sociaux |
| | Vécu spécifique | Habitude | Habitude |
| **Eléments secondaires** | Conscience professionnelle, Professionnalisme | Devoir | Théorie des liens sociaux |
| | C'est logique, c'est un fait | Motivation intrinsèque | Modèle motivation |
| | Culture d'entreprise | Normes subjectives | TPB |
| | Prise de conscience collective | Normes subjectives /Croyances | TPB / Liens sociaux |
| | Influence du dirigeant / hiérarchie | Normes subjectives /Croyances /Support dirigeant | TPB / Liens sociaux /TMS |
| | Reflexe, Naturel, Machinal, habitude | Habitude / Routinisation | Habitude |
| | Existence d'une charte | Efficience liée à l'implication des décideurs | Codes d'éthique / TMS |
| | Sinistres précédents | Effet Vaccin / Sensibilisation | Perception des menaces |
| | Priorisation travail habituel / Sécurité | Implication | Théorie des liens sociaux |
| **Freins** | | **Construits** | |
| | Difficulté d'accès au support | Conditions facilitatrices | UTAUT |
| | Pénibilité | Attitudes envers le comportement/effort attendu | TPB |
| | Pas de perception du risque | In-utilité perçue ? | TAM / UTAUT |
| | Complexité de la tâche | Complexité /Maîtrise perçue /Facilité d'utilisation | TPB/TAM |
| | Ce n'est pas mon problème => Informaticiens | Croyances / Déni / Evitement | Liens sociaux / Emotion |

**Tableau 3. Correspondance entre les théories incluses dans les questionnaires et les éléments extraits des entretiens**. Adapté de ma thèse (2006).

Ce tableau est important pour la suite, car il a conditionné mes travaux ultérieurs, notamment pour mes choix de construits et de certaines variables de contrôle dans mes études quantitatives basées sur les théories du coping. Il met aussi en évidence l'importance de l'habitude, de la préservation de la vie privée (privacy concern) et des normes subjectives. On remarque enfin l'influence du dirigeant et celle de son autorité hiérarchique, que je rattacherai plus tard au courant théorique du 'top management support' (TMS), qui sera détaillé dans la seconde partie de ce mémoire.

Deux autres éléments sont à souligner : premièrement, si j'avais exploité à l'époque la connaissance des 'sinistres précédents' dans mes entretiens, cette sinistralité s'est avérée importante pour la formation de l'émotion 'peur' ou de la perception d'une menace, au travers de la vulnérabilité (probabilité) et de la sévérité (impact) perçues des sinistres potentiels. Cette appréciation des menaces a été utilisée dans les théories du coping (Lazarus, 1966) et plus particulièrement dans la PMT (Rogers, 1983). La PMT intègre d'ailleurs également l'efficacité personnelle (self-efficacy) et l'efficacité de la réponse (response efficacy) que l'on retrouve dans les freins, en bas du tableau 3, reflétant la pénibilité, la complexité et l'inutilité de prendre des mesures de sécurité. Pour mémoire, la PMT n'a été adaptée des travaux de psychologie clinique et appliquée à la sécurité de l'information qu'à partir de 2008 par Workman et ses collègues, soit deux ans après la soutenance de ma thèse.

Deuxièmement, la pertinence de la théorie de la dissuasion n'est pas ressortie de mes entretiens. Des travaux ont montré que cette théorie avait des résultats variables selon la culture (D'Arcy & Herath, 2011; Hovav et D'Arcy, 2012; Hu *et al.*, 2011; Thèse, 2006). Une autre explication tient à la rareté du poste de DSI (surtout à plein temps) en PME, ce qui fait que l'arsenal nécessaire à la détection des fautes et à leur punition n'avait été mis en place dans aucune des 9 entreprises que j'avais étudiées en 2005. Ce fait est important, car dans la suite de mes travaux, j'ai sciemment écarté les comportements de 'compliance' pour m'intéresser à la mise en place *volontaire et libre* des mesures de sécurité.

Deux articles ont été tirés de cette thèse et ont été publiés dans SIM, en 2008 pour les résultats généraux concernant les dirigeants et salariés et en 2012 pour une analyse plus approfondie des résultats, recentrée sur les dirigeants.

### *1.1.3. Publications et travaux découlant de la thèse*

Les travaux relatifs à ma thèse ont été présentés lors de plusieurs colloques de l'association information et management (AIM). Dans un premier temps, lors des conférences AIM 2005 puis 2008 et 2009, ce qui a mené à un premier article publié dans SIM fin 2008, et dans un second temps en 2011 pour finaliser le second publié dans SIM quatre ans plus tard.

#### *1.1.3.1. L'article de SIM 2008*

Cette recherche s'intitule « *une étude des comportements liés à la sécurité des systèmes d'information en PME* » et a été publiée dans Systèmes d'Information et Management, volume 13, n°4, p. 7-30.

Cet article résume mon travail de thèse et répond à la question de recherche « *quels sont les déterminants des comportements liés à la sécurité des systèmes d'information dans les PME ? »*. Il discute de l'adaptation de modèles traitant des théories sur les comportements d'acceptation et/ou d'utilisation des TIC ainsi que certaines théories tirées de la psychologie ou la criminologie. Cette discussion permet d'énoncer trois propositions de recherche concernant les dirigeants et salariés, qui sont ensuite confrontées au terrain par le biais d'une étude qualitative auprès de 29 acteurs en PME. L'étude qualitative a permis de confirmer ces propositions et a fait apparaître la spécificité des comportements relatifs à la SSI.
Au travers de huit études de cas, j'ai interrogé le dirigeant, la personne en charge du SI ou de la SSI si elle existait, ainsi que des salariés et/ou cadres pour chaque entreprise.
Un guide d'entretien semi-directif a été constitué pour chaque type d'acteur, comportant sept thèmes principaux, tels que la vision de la sécurité, les rôles déclarés, les facteurs d'implication et d'action et les freins ou encore les sinistres vécus. Les discours ont été triangulés (Klein et Myers, 1999) dans le but de vérifier le partage des rôles et qui était le véritable instigateur des actions mises en place. Les entretiens ont été enregistrés puis retranscrits ce qui a conduit à plus de 200 pages de textes à analyser. Des fiches d'entretiens comportant des éléments sur le contexte et une visite complète de l'entreprise ont complété les informations enregistrées. Un ensemble d'analyses de discours ont été réalisées en accord avec la méthodologie proposée par Miles et Huberman (2003) : trois matrices interentreprises (une par type d'acteur) et huit matrices intra-entreprises ont été créées. Les étapes de codage et d'analyse ont nécessité au total la création de vingt-quatre tableaux d'analyse, soit pour condenser les données (Miles et Huberman, 2003) afin de détailler un thème précis, soit pour croiser certaines informations (Klein et Myers, 1999).
Les principaux résultats concernent les salariés et sont visibles dans le tableau 3. Sur un plan théorique, les principales contributions sont : Premièrement, au sujet des salariés, j'ai pu constater que les comportements en SSI allaient au-delà de la technique et de l'acceptation des technologies. De ce fait, des construits tels que l'utilité perçue ou l'efficacité perçue n'ont qu'une influence limitée sur les comportements relatifs à la SSI, sauf dans le cas d'une trop grande complexité, qui va freiner l'exercice de certaines actions de sécurité techniques. Le seul construit des théories de l'acceptation dont j'ai pu constater l'effet est l'influence sociale (ou normes subjectives, voir tableaux 1 et 3). Ce résultat semble logique, dans la mesure où un employé peut être influencé dans ses comportements relatifs à la sécurité par ses collègues ou son dirigeant, ce qui a d'ailleurs été confirmé dans de nombreux articles sur la sécurité de l'information par la suite (Herath et Rao, 2009 ; Lee et Larsen, 2009 ; SIM, 2017 ; SIM, 2019).

Pour les autres théories (voir tableau 2), les éléments qui ont le plus d'effet sont rattachés à la motivation intrinsèque et aux liens sociaux (attachement, devoir, identification).
Deuxièmement, concernant les dirigeants, les résultats obtenus sont en phase avec les éléments ressortant de l'étude de la littérature : la mauvaise perception des risques encourus, la difficulté de l'évaluation de la valeur des informations sous forme électronique, l'importance du rôle du dirigeant dans la prise en compte des problématiques liées à la SSI et l'influence du dirigeant sur les comportements des salariés.
Sur un plan managérial, ces résultats peuvent servir à mettre en place une sensibilisation et une mise en garde des dirigeants au sujet de la délégation, qui peut s'avérer risquée et doit donc être réalisée en prenant des précautions (contrôles réguliers, clarté des contrats, etc.). De la même manière, l'influence bénéfique des dirigeants sur les comportements des salariés a été confirmée, cette influence doit donc être mise en avant et développée. Enfin, l'automatisation de certaines tâches relatives à la sécurité (sauvegardes, mises à jour…) ainsi que l'amélioration du support et de l'aide aux utilisateurs limitera l'aspect complexe et fastidieux que peuvent représenter certains comportements en SSI.
Si cet article était en majeure partie un résumé de ma thèse, celui qui a été publié quatre ans plus tard dans SIM en 2012 correspondait à une nouvelle analyse plus approfondie (1) des motivations du dirigeant de PME à s'impliquer dans la SSI de son entreprise, (2) des types d'actions qu'il exerce, et (3) de ses interactions avec son salarié en charge de la SSI, le plus souvent à temps partiel.

#### *1.1.3.2. L'article SIM 2012*

Cet article s'intitule « *Implication et action des dirigeants : quelles pistes pour améliorer la sécurité de l'information en PME* » et a été publié dans Systèmes d'Information et Management, volume 17, n°2, p. 115-149.

Cette recherche, basée sur étude exploratoire, visait à répondre à la question suivante : « *Comment améliorer le rôle du dirigeant dans la SSI de sa PME ? »* Pour traiter cette question, j'ai étudié (1) les facteurs conditionnant leur implication et leurs actions, (2) les conséquences de leur implication et de leurs actions sur le niveau de sécurité de l'entreprise, (3) comment les rôles sont partagés dans la gestion de la SSI entre les divers acteurs.

Ce travail était basé sur la même méthodologie qualitative que l'article précédent. J'ai repris les entretiens et approfondi mes analyses afin d'étudier l'implication du dirigeant, qui peut se traduire par des actions directes ou indirectes. Les actions directes correspondent à la gestion des problèmes de sécurité ou la mise en place de mesures de sécurité par le dirigeant lui-même. Le concept d'actions indirectes est proche du 'top management support' (TMS) (Dong *et al.,* 2009 ; Gottschalk, 1999 ; Liang *et al.*, 2007 ; McComb *et al.*, 2008). Un dirigeant de PME pourra mettre l'accent sur la sécurité de l'information lors de communications orales plus ou moins informelles (Jarvenpaa et Ives, 1991), ou valoriser, encourager, ou recruter des responsables de la SSI (Ragu-Nathan *et al.*, 2004 ; Indihar Štemberger *et al.*, 2011). Le dirigeant pourra mettre en place un 'contexte de soutien' dans l'organisation (Ragu-Nathan *et al.*, 2004) car il a été montré que le soutien de la direction est essentiel dans l'obtention d'une adhésion des employés à la SSI (Avolio, 2000 ; Johnston et Hale, 2009). L'implication pourra enfin soutenir la perception par le dirigeant des propositions du personnel en charge du S.I. (Jarvenpaa et Ives, 1991).

Mes résultats ont montré que l'implication du dirigeant est influencée par son passé personnel et professionnel et par son attachement à son entreprise. De plus, conformément à Jarvenpaa et Ives (1991), les croyances au sujet des pertes qu'ils pourraient subir, la perception d'une forte concurrence et le niveau de connaissances en S.I. vont influencer de manière positive l'implication des dirigeants dans la SSI de leur entreprise.

Concernant les actions des dirigeants, la perception de la priorité d'autres actions va limiter voire bloquer leurs actions directes. De plus, si le dirigeant peut se reposer sur une tierce personne, il agira moins de manière directe, même s'il est impliqué. Enfin, j'ai aussi mis en évidence que l'obligation de respecter des normes ou méthodes aura un effet fort sur les actions directes du dirigeant, mais deux éléments vont relativiser son intérêt : premièrement peu de PME sont soumises à de telles obligations et, deuxièmement, la norme ou méthode à respecter ne sera pas forcément spécifique à la SSI et ne couvrira donc pas systématiquement toutes les actions à mettre en place.

La figure 3 ci-dessous met en évidence les quatre situations ainsi que les types d'actions, directes ou indirectes, qui s'y rattachent :

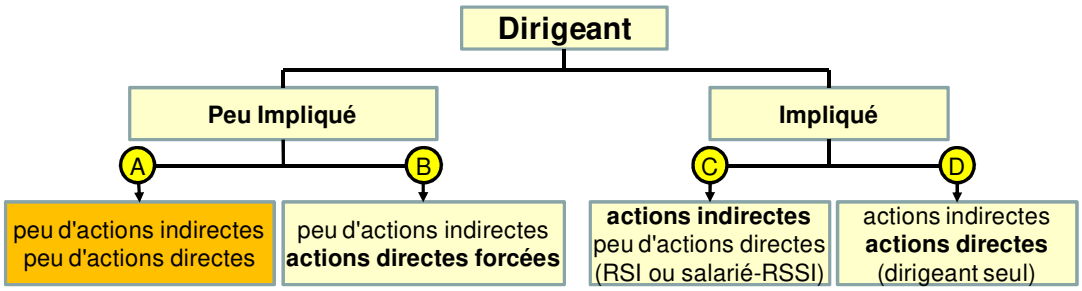


**Figure 3. Les actions directes et indirectes selon la situation (SIM, 2012)**

Dans la situation 'A', si personne ne peut compenser le manque d'actions du dirigeant, le niveau de sécurité de l'entreprise est potentiellement très faible (pas de firewall, pas d'antivirus, pas de sauvegardes ni de mots de passe, aucune procédure). Dans la situation 'B', le dirigeant va manquer d'actions indirectes car il ne sera pas impliqué, et n'effectuera que des actions directes 'forcées' liées aux éléments obligatoires de la ou des normes qu'il aura dû implémenter. Dans cette situation, le dirigeant n'est pas en recherche d'informations relatives à la SSI qui pourraient le sensibiliser et le motiver. Dans la situation 'C', un niveau faible d'actions directes du dirigeant sera compensé par une tierce personne (salarié en charge de la SSI). Ce sera surtout la sensibilisation du dirigeant à la nécessité de mener des actions indirectes qui va compter. Dans la situation 'D', le dirigeant va agir à la fois de manière indirecte et directe, les seules limites seront liées à l'échelle de ses priorités. Son niveau technique ne sera pas véritablement un handicap car il pourra acquérir des connaissances supplémentaires grâce à ses interactions avec son prestataire extérieur. Comme le dirigeant est impliqué, il sera possible d'agir sur sa perception des priorités par une sensibilisation complémentaire aux pertes possibles par exemple. Il sera aussi possible de développer les connaissances en SI et en SSI du dirigeant, par le biais d'une formation par exemple, dans l'optique d'améliorer sa réflexion stratégique pour arriver à mieux lier stratégie d'entreprise et SSI.

Dans l'étude du partage des rôles entre les divers acteurs en entreprise, j'ai identifié le rôle de 'salarié-RSSI', correspondant au fait que quand le dirigeant n'était pas impliqué (situations de type 'A'), même si le dirigeant n'agissait pas ou très peu, à chaque fois un salarié prenait malgré tout en charge le S.I. de l'entreprise et sa sécurité. Les divers salariés-RSSI rencontraient des problèmes similaires : ils ne sont pas soutenus par leur dirigeant, ce qui entraîne que leur position hiérarchique n'est pas affirmée. De plus, la fonction du salarié-RSSI étant informelle, il n'est aux yeux de tous qu'un salarié comme les autres. Enfin, n'ayant pas de diplôme spécifique pour légitimer leurs compétences, le salarié-RSSI ne dispose ni de l'autorité ni de la crédibilité nécessaires pour assurer correctement sa fonction.

Sur un plan théorique, l'identification d'un salarié-RSSI, qui assume de manière informelle la responsabilité du SI de son entreprise et de sa sécurité a ouvert un nouveau champ d'étude. Les

conditions d'apparition de salariés-RSSI, l'identification des problématiques qu'ils rencontrent et leur résolution conduisent à de nombreuses pistes de recherches futures.

Une autre contribution de ce travail est l'exploration des relations entre l'implication du dirigeant en SSI et ses actions directes et indirectes, peu étudiées dans la littérature en systèmes d'information. J'ai montré que l'implication du dirigeant prend le pas sur les actions, dans l'obtention d'un bon niveau de SSI pour l'entreprise. Les actions indirectes, notamment la manière dont le dirigeant va interagir avec son RSI ou le salarié-RSSI, ainsi que l'influence qu'aura le dirigeant sur ses salariés, sont les plus critiques.

Sur un plan managérial, mon travail a identifié les facteurs d'implication et d'action des dirigeants, qui pourront être intégrés à des sensibilisations et formations pour leur donner plus d'impact. Cette étude a aussi permis de mieux comprendre comment se partagent les rôles en matière de SSI dans les PME. J'ai aussi mis en évidence l'importance d'une meilleure gestion du salarié en charge de la SSI, notamment lorsque cette prise en charge est informelle. Si c'est un salarié-RSSI, il faudra en plus s'assurer d'une bonne collaboration entre les acteurs et améliorer les tâches du salarié-RSSI. Une formation complémentaire ou une validation des acquis assiéra mieux ses compétences techniques, tandis qu'un aménagement plus formel de son travail (part de sa charge en SSI comparée à son métier 'officiel') et/ou une valorisation de sa tâche faciliteront sa reconnaissance dans l'entreprise.

Ma conclusion de 2012 soulignait l'importance de prendre en compte les aspects 'SSI obligatoire' que peuvent présenter certaines normes ou législations. L'utilisation des normes de SSI, parmi les PME de moins de 200 salariés, s'avère malheureusement rare car elles sont en général trop lourdes pour de petites structures (HICSS, 2008). A défaut de normes, pour adopter de bonnes pratiques, les dirigeants de PME pourraient être informés de l'existence de guides explicitant la mise en place de ces bonnes pratiques (ex : site de l'ENISA). La voie juridique est aussi prometteuse, car des lois pourraient obliger les dirigeants, même non impliqués, à mettre en place les actions les plus indispensables.

Ces articles publiés dans SIM en 2008 et 2012 ont servi de base pour de nombreux travaux ultérieurs. Comme évoqué dans la conclusion du papier de 2012, des études quantitatives ont permis d'approfondir certains des facteurs de motivation pour exercer ou implémenter de meilleures pratiques ou pour la mise en place de mesures de sécurité, tant pour les salariés que pour les dirigeants.

Par exemple, l'article SIM de 2008 a mis en évidence la préservation de l'intimité, qui a été réutilisée dans mes articles sur le BYOD (en tant que 'privacy concern'). De même, la notion d'habitude a été reprise dans notre communication AIM en 2015, même si nous n'avons pas pu l'intégrer dans l'article SIM de 2017, faute de résultats saillants. Cependant, l'influence sociale a pu être utilisée avec succès dans de nombreux travaux par la suite. Dans le chapitre consacré aux projets (cf. §2.1), il est aussi envisagé d'utiliser la théorie des liens sociaux dans une prochaine étude.

L'article SIM de 2012 mettait en évidence l'importance du top management support (TMS) ainsi que les comportements directs et indirects que nous avons réutilisés dans notre article qui vient d'être publié dans SIM, 2019.

Quelques temps après, fin 2014, j'ai découvert la protection motivation theory (PMT), qui faisait parfaitement écho à mes travaux sur l'implication du dirigeant dans la SSI, dans les articles de 2008 et 2012. Ceci m'a permis de continuer mes travaux en utilisant des méthodologies quantitatives, ce qui a donné lieu à de nombreuses communications et articles, et s'avère, à ce jour encore, la source de nouveaux projets.

Le tableau 3 a permis de faire un point sur l'adaptation et la pertinence des construits mobilisés dans le cadre de ma thèse au contexte des comportements en matière de SSI. Nous allons

examiner dans la partie suivante les limitations des modèles théoriques vus précédemment pour une utilisation dans le contexte de la SSI.

### *1.1.4. Limitations des théories précédentes : vers la théorie du Coping de Lazarus*

#### *1.1.4.1. Limitations des théories précédentes*

Les théories présentées dans le paragraphe 1.1.1, si elles se sont avérées utiles dans une première approche, restent basées sur les courants classiques de l'acceptation et de l'adoption des technologies et visent principalement à expliquer une intention comportementale, alors que les comportements relatifs à la sécurité de l'information correspondent plus à des réactions face à des évènements menaçants (Workman *et al.*, 2008).

En sécurité de l'information, la littérature est majoritairement anglo-saxonne (Moody *et al.*, 2018). Dans cette littérature, les théories basées sur le respect ('compliance') des règles et chartes de sécurité occupent une grande place dans ces recherches et de nombreuses recherches ont intégré des construits basés sur la théorie générale de la dissuasion (general deterrence theory, d'Arcy *et al.*, 2011) et certaines théories proches (Moody *et al.*, 2018), telles que la théorie de la neutralisation et la control balance theory (CBT).

Pourtant, en amont de la 'compliance', des règles et chartes de sécurité, ainsi que des mesures de sécurité, doivent être mises en place. Dans une entreprise, ces mesures ou chartes n'existeront que si les projets de la DSI sont validés et financés par la direction, et s'il n'y a pas de DSI, l'implication de la direction devra être encore plus grande pour décider et s'assurer de cette mise en place. En conséquence, le directeur de l'entreprise occupe une place majeure dans la sécurité des informations de l'entreprise, notamment en PME, ce que j'ai d'ailleurs montré dans mes articles dans SIM en 2008 et 2012.

Afin de mieux comprendre les motivations et les comportements des dirigeants mis en évidence dans ces études qualitatives, je me suis orienté vers des approches quantitatives, basées sur des modèles utilisés en psychologie. Dans le domaine de la sécurité de l'information, certaines approches permettent de prendre en compte les aspects 'menaces' ainsi que la capacité à gérer un évènement menaçant : elles sont basées sur la théorie du 'coping' de Lazarus (1966).

#### *1.1.4.2. La théorie du coping de Lazarus*

Remonter à la théorie initiale permet de mieux comprendre comment ont été conçues les autres théories que nous examinerons par la suite et de mieux en appréhender les forces et faiblesses, ainsi que les possibilités de les enrichir, dans le cadre des comportements relatifs à la sécurité des informations. La théorie du coping postule que certains évènements vont être suffisamment importants pour déclencher des comportements d'adaptation basés sur deux sous-processus clé, l'appréciation primaire de l'évènement et l'appréciation secondaire du comportement de coping (voir figure 4).

Ces événements appartiennent à deux types principaux : les défis, qui sont perçus comme pouvant avoir des conséquences positives, et les menaces, perçues comme pouvant avoir des conséquences négatives. Les événements vont généralement être perçus à la fois comme des défis et des menaces (Lazarus et Folkman, 1984).

L'*appréciation primaire* correspond à l'évaluation des enjeux et des conséquences potentielles de l'évènement (menaces, opportunités ou les deux) et leur significativité pour l'individu (Folkman, 1992) et résulte en une émotion anticipative (Lazarus, 1991).

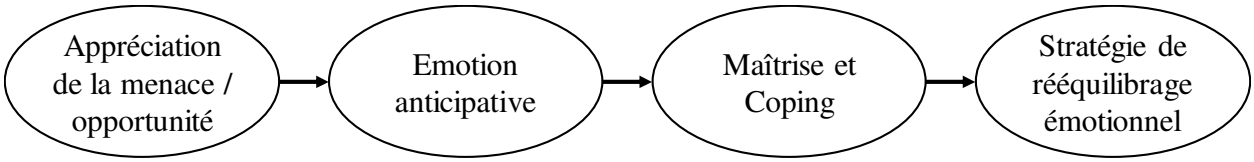


**Figure 4. Modèle théorique du coping (adapté de Lazarus, 1991)**

*L'appréciation secondaire* (ou *coping appraisal)* est l'évaluation des options disponibles qui va guider le choix de *stratégies* de *coping* par l'individu, qui vont permettre de rééquilibrer, au moins en partie, le décalage émotionnel provoqué par l'évènement. Ces options vont dépendre du niveau de contrôle que l'individu pense pouvoir exercer sur la situation et ce qu'il pense pouvoir faire à cet égard, compte tenu des ressources d'adaptation à sa disposition (Lazarus et Folkman, 1984). Les options sont diverses, telles que le fait de modifier la situation, de l'accepter, de mieux s'informer, ou éviter d'agir de manière impulsive et contre-productive.

Le coping est défini comme « les *efforts cognitifs et comportementaux exercés pour gérer des nécessités internes et/ou externes spécifiques qui sont ressenties comme mettant à l'épreuve ou excédant les ressources de la personne »*[4] (Lazarus et Folkman, 1984, p.141). Le coping va jouer deux rôles de régulation des émotions stressantes : soit par une *réappréciation cognitive* de la situation (adaptation centrée-émotion), soit par une *action* sur la relation personne-environnement perturbée par l'événement à l'origine du stress (adaptation centrée-problème).

Les stratégies de coping *centrées-émotion* correspondent à une modification de la perception de la situation, mais ne modifient pas le problème en lui-même. Elles sont uniquement orientées vers soi et vont inclure l'acceptation passive ou le fait d'éviter la situation, le déni (de l'évènement, de la situation ou de ses conséquences), le fait de percevoir les conséquences des menaces comme faibles, la comparaison positive ('les autres vivent des situations pires'), l'évacuation des émotions négatives et enfin la recherche d'un soutien psychologique ou émotionnel (Folkman *et al.* 1986 ; Lazarus et Folkman, 1984).

Les stratégies de coping *centrées-problème* visent à gérer le problème perturbateur lui-même. Elles vont traiter des aspects spécifiques de la situation en 'se modifiant soi-même' ou bien en modifiant l'environnement. On pourra *changer son comportement* en adoptant de nouvelles normes comportementales, en apprenant de nouvelles compétences ou procédures, ou en changeant ses aspirations. Les *actions sur l'environnement* serviront à diminuer les pressions environnementales ou les obstacles, à réaffecter certaines ressources ou à modifier des procédures (Lazarus et Folkman, 1984).

La stratégie de coping a pour but de réguler les émotions et les tensions personnelles, de rétablir ou maintenir un sentiment de stabilité, ou enfin de réduire la détresse émotionnelle (Lazarus et Folkman, 1984). Les individus auront tendance à choisir la stratégie la plus susceptible de réussir et le choix d'une stratégie de coping centrée-émotion ou centrée-problème dépendra du niveau de maîtrise (contrôle) du comportement de coping par l'individu.

Quand les individus ont le sentiment d'avoir une *maîtrise limitée* de la situation, ils choisiront plutôt une stratégie de coping centrée-émotion (Folkman, 1992 ; Folkman *et al.*, 1986 ; Lazarus et Folkman, 1984). Dans ce cas, adopter une stratégie centrée-problème aura peu de chances d'avoir un effet sur le problème, ce qui aboutira à plus de frustration et de détresse (Folkman, 1992). A l'inverse, quand les individus pensent avoir une *bonne maîtrise* de la situation, ils

[4] "*The cognitive and behavioral efforts exerted to manage specific external and/or internal demands that are appraised as taxing or exceeding the resources of the person."*

choisiront une stratégie de coping principalement centrée-problème. Ici, adopter une stratégie centrée-émotion risquerait d'aboutir à des frustrations (Folkman, 1992).

Pour les détails des comportements résultant des stratégies, il était clair que les chercheurs devaient choisir des éléments d'adaptation pertinents pour le contexte et la transaction individuelle en question (Lazarus et Folkman, 1984), car l'adaptation est un processus transactionnel entre un individu et une situation spécifique. Le processus de coping peut se dérouler avant que l'événement ne se produise réellement (la période d'anticipation), au moment où l'événement se produit (la période d'impact), ou enfin après l'événement (période post-impact) (Folkman, 1992).

Les travaux de Lazarus ont servi de base pour aboutir à deux grandes familles de théories. La première famille correspond à la prise en compte des menaces et des stratégies centrées-problème, qui a été utilisé dans le cadre notamment de la protection motivation theory (PMT) de Rogers (1975 ; 1983), et la deuxième correspond à un modèle bien plus large, le coping model of user adaptation (CMUA) de Beaudry et Pinsonneault (2005), qui sera traité dans la partie 1.3.

## 1.2. Protection motivation theory (PMT) et théories associées

La théorie de la motivation à la protection ou PMT a été élaborée par Rogers en 1975 dans le domaine de la psychologie clinique, en partant du principe que des changements d'attitude peuvent être déclenchés par des 'appels à la peur' (fear appeals). Son but était d'éliminer les schémas de réponse pouvant avoir des conséquences néfastes ou d'établir des schémas de réponse pouvant empêcher la survenue d'événements menaçants. Sa théorie initiale prenait en compte les concepts suivants : la gravité des menaces (impact potentiel), la vulnérabilité perçue à la menace (probabilité), l'inquiétude suscitée par la menace, la disponibilité et l'efficacité de la réaction de coping, pour réduire ou éliminer la probabilité de cet événement menaçant. Selon Rogers, ces éléments conduisent à une motivation pour adopter (ou non) les réponses recommandées.

Les sources d'information à l'origine des processus d'évaluation cognitive peuvent être environnementales (par exemple, des appels à la peur sous forme verbale ou observation de ce qui arrive à d'autres) ou intrapersonnelle (par exemple, des expériences antérieures de menaces similaires, ainsi qu'un feedback sur le résultat des comportements de coping antérieurs).

A ma connaissance, les premiers à avoir utilisé la PMT en sécurité de l'information sont Workman et ses co-auteurs en 2008. Actuellement, la PMT est considérée comme la théorie de référence pour expliquer les comportements relatifs à la SSI (Williams *et al.*, 2014). Des formes proches de la PMT ont aussi été adaptées au contexte de la SSI (Boss *et al.*, 2015 ; Crossler *et al.*, 2014 ; Siponen *et al.*, 2014) : On trouve la théorie de l'évitement des menaces technologiques (TTAT) ou 'Technology Threat Avoidance Theory' (Liang et Xue, 2009), les appels à la peur (Johnston et Warkentin, 2010) et le modèle de croyance en matière de santé (HBM) ou 'health belief model' (Ng *et al.*, 2009). Nous allons nous focaliser sur la PMT, qui a été adoptée pour nos travaux décrits plus loin.

La PMT est basée sur deux processus d'évaluation successifs qui conditionnent la motivation des individus à s'engager dans un comportement protecteur (Maddux et Rogers, 1983 ; Sommestad *et al.*, 2015). Ces processus sont l'appréciation primaire des menaces (threat appraisal) et l'appréciation du comportement de coping à exercer (coping appraisal).

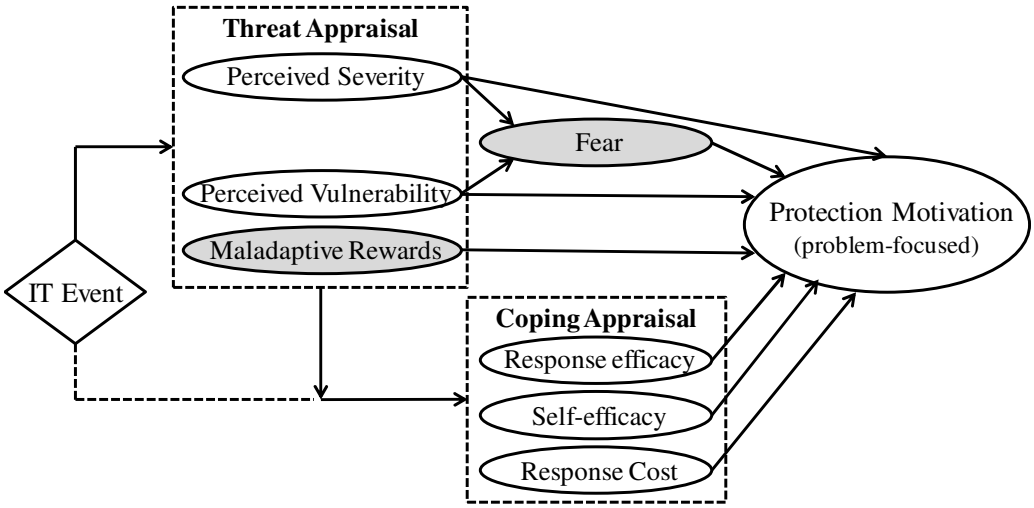


**Figure 5. La protection motivation theory (Full PMT)**
Adapté de Rogers (1983) et Boss *et al.* (2015)

La PMT contient des construits qui peuvent varier selon le référentiel qui a été utilisé. Son appellation va alors être différenciée, pour caractériser les quatre variantes de la PMT.

La première typologie distingue la **'full' PMT** qui intègre dans le modèle la mesure d'un construit représentant la peur ressentie ('fear'), ainsi que les 'maladaptive rewards', c'est-à-dire les bénéfices réalisés *lorsque l'on n'adopte pas* les comportements de coping nécessaires (Boss *et al.*, 2015), et la '**core' PMT**, qui correspond au modèle le plus classique (voir la partie non grisée en figure 5 ci-dessus).

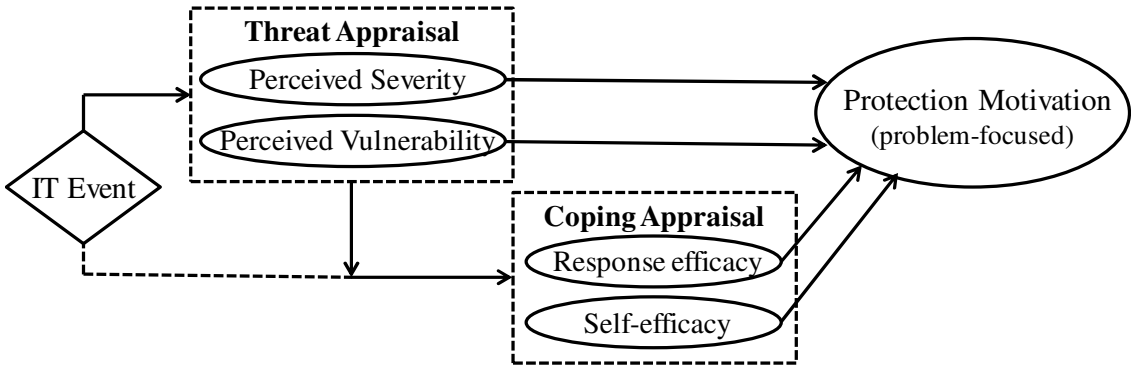


**Figure 6. La protection motivation theory (PMT)**
Adapté de Rogers (1983) et Moody *et al.* (2018)

La deuxième typologie distingue la **PMT** (équivalente à la 'core' PMT sans le 'response cost', voir figure 6 ci-dessus) de la **PMT étendue** qui rajoute le 'response cost' et les 'maladaptive rewards', sans toutefois intégrer la peur (Moody *et al.*, 2018). Je pense que cette typologie est plus adaptée que la 'full' PMT, car Rogers a révisé sa PMT originelle en relativisant l'impact des appels à la peur. En effet, selon Rogers (1983, p. 158) : « *le changement d'attitude ne résulte pas d'un état de peur émotionnel* », mais dépend de l'ampleur de la motivation à la protection suscitée par « *le processus d'évaluation cognitive d'un événement perçu comme menaçant et susceptible de se produire, en combinaison avec la croyance qu'une réaction d'adaptation appropriée peut effectivement empêcher l'événement menaçant de se produire* ».

Mes travaux se sont donc basés sur la 'core' PMT ; je vais donc maintenant détailler les processus cognitifs d'appréciation primaire des menaces puis l'appréciation secondaire de 'coping appraisal', dans ce cadre conceptuel.

### *1.2.1. Appréciation primaire des menaces*

L'appréciation des menaces (threat appraisal) est définie comme l'anticipation d'une atteinte psychologique, sociologique ou physique ou d'un préjudice causé à soi-même ou à autrui (Workman *et al.*, 2008). Les personnes qui perçoivent cette menace ajusteront leur comportement en fonction du risque qu'elles sont disposées à accepter. Ce processus d'appréciation de la menace est basé sur deux facteurs (Rogers, 1983) qui réduisent la probabilité d'apparition d'une réponse inadaptée, c'est-à-dire un comportement indésirable destiné uniquement à atténuer la peur (nier la menace, par exemple). Ces facteurs sont la vulnérabilité perçue et la sévérité perçue.

La "*sévérité*" perçue de la menace fait référence à des lésions corporelles mais peut également impliquer des menaces intrapersonnelles telles que l'estime de soi ou des menaces interpersonnelles telles que les relations de travail. En SSI, ce facteur représente l'impact potentiel (Vance *et al.*, 2012, p. 192) de la concrétisation d'une menace, parce que les mesures de sécurité en place se seront avérées insuffisantes ou inefficaces (Ifinedo, 2012 ; Liang et Xue, 2009). La sévérité inclut par exemple, le niveau perçu d'une perte d'activité, la perte de données, des pertes financières et des effets secondaires potentiels (par exemple, une perte d'image).

Le second facteur est la "*vulnérabilité*" perçue, c'est-à-dire la probabilité conditionnelle qu'un évènement menaçant se concrétise (Rogers, 1983), si l'on considère qu'aucun comportement d'adaptation n'est engagé ou qu'un comportement existant n'est pas adapté pour limiter cette vulnérabilité (Lee et Larsen, 2009).

L'augmentation de la sévérité perçue et de la vulnérabilité perçue va conduire à une plus grande intention comportementale de se protéger. Ce processus d'appréciation de la menace est complété par un processus d'évaluation de la capacité à répondre, appelé 'coping appraisal'.

### *1.2.2. Appréciation secondaire du comportement de coping*

Cette appréciation secondaire aura une influence qui va dépendre du *contrôle perçu* par un individu vis-à-vis du comportement nécessaire, de ses capacités perçues et des efforts qu'il déploiera pour mener à bien ce comportement (Bandura, 1977). En SSI, cela pourra correspondre à la perception par un individu de sa capacité à faire face à une menace, voire à la prévenir. Selon Rogers (1983), trois composantes vont influer sur cette appréciation : l'efficacité que la réponse pourra avoir, l'efficacité personnelle de l'individu et le coût que représentera la réponse.

*L'efficacité de la réponse* correspond à la croyance par l'individu que la réponse comportementale qu'il va adopter sera efficace, ou aura des conséquences bénéfiques (Rogers, 1983). Dans nos travaux, cela reflète la capacité, perçue par l'individu, d'implémentation de mesures relatives à la sécurité de l'information. Il a été démontré que l'efficacité de la réponse a un effet sur les intentions de se protéger, de protéger les autres, ainsi que sur le comportement déclaré par un individu. L'efficacité de la réponse se combine à la vulnérabilité perçue, pour agir sur l'intention d'adopter le comportement adéquat. A l'inverse, si la réponse est perçue comme ineffective, une augmentation de la vulnérabilité perçue se traduira par une forte baisse de l'intention d'adopter le comportement. Par conséquent, dans certaines situations, un niveau d'efficacité de réponse insuffisant peut réduire considérablement l'effet exercé par les menaces perçues.

En plus de relativiser l'impact de 'l'appel à la peur' sur la motivation à la protection, l'efficacité personnelle était la principale nouvelle composante de la théorie révisée de Rogers, en 1983. *L'efficacité personnelle* est définie comme « *les croyances des individus en leur capacité à atteindre des niveaux adéquats de performance afin d'exercer une influence sur les évènements qui affectent leurs vies* » (Bandura, 1994, p. 81). Elle correspond donc à la perception par l'individu qu'il peut exercer avec succès une 'coping response'. L'efficacité personnelle détermine si un comportement d'adaptation sera adopté ou non, quel comportement sera choisi et quel effort sera déployé (Bandura, 1977 ; Rogers, 1983).

Rogers (1983) et Maddux et Rogers (1983) ont montré que l'efficacité personnelle avait un effet significativement positif sur l'intention d'adopter des comportements de protection, dans de nombreuses études sur la PMT. En outre, de nombreuses expérimentations ont mis en évidence le fait que si l'efficacité de la réponse ou l'efficacité personnelle est élevée, l'augmentation de la gravité ou de la vulnérabilité aura un effet principal simple sur les comportements de protection. A l'inverse, quand l'efficacité de la réponse ou l'efficacité personnelle est faible, l'augmentation de la gravité ou de la vulnérabilité n'aura aucun effet, ou aura un effet inverse, réduisant ainsi la motivation à la protection (Rogers, 1983). En SSI, l'individu se demandera si la mise en œuvre de mesures liées à la sécurité de l'information pourra améliorer la sécurité de son entreprise et réduire les failles de sécurité.

L'efficacité perçue de la réponse et l'efficacité personnelle doivent l'emporter sur le coût de la réponse pour déclencher une réaction d'adaptation.

*Le coût de la réponse* a été ajouté par Rogers dans sa PMT révisée. Le coût de la réponse fait référence aux efforts physiques et cognitifs qui entrent en jeu dans la réponse adaptative (Liang et Xue, 2010). Ils correspondent aux inconvénients, dépenses, désagréments, difficultés, complexité et effets secondaires de l'abandon des comportements habituels au profit de nouveaux comportements plus adaptés. En SSI, cela peut correspondre à l'argent ou au temps nécessaire à investir dans le comportement ou la mesure de sécurité, ou encore aux inconvénients ou difficultés découlant du comportement lui-même.

Les processus d'appréciation primaire (threat appraisal) et secondaire (coping appraisal) déterminent si un comportement de coping sera initié, quels comportements seront choisis et quels efforts seront exercés (Bandura, 1977 ; Rogers, 1983). Ils conduiront à une réponse adaptative, appelée aussi ajustement comportemental, correspondant à la fameuse 'motivation à la protection' qui a donné son nom à la protection motivation theory.

### *1.2.3. Les comportements de coping*

La PMT résulte en une « *décision (ou intention) d'initier, de poursuivre ou d'inhiber les réponses adaptatives applicables (ou les comportements d'adaptation)* » (Floyd *et al.*, 2000, p. 411). Même si PMT suppose que *« la motivation à la protection est mieux mesurée par des intentions comportementales »* (Rogers, 1983, p. 172), cette théorie « est suffisamment générale pour s'appliquer à toute situation impliquant une menace » (Rogers, 1983, p. 172), c'est-à-dire, qu'elle permet d'étudier des comportements correspondant à des actes uniques, répétés ou de nature multiple (Prentice-Dunn et Rogers, 1986). Par conséquent, en fonction du type de comportement examiné, plusieurs axes de recherche basés sur la PMT ont exploré - de manière équilibrée (voir Annexe 2) - l'intention comportementale (Moody *et al.*, 2018 ; Tsai *et al.*, 2016 ; Tu *et al.*, 2015), le comportement réel (Chen et Zahedi, 2016 ; Posey *et al.*, 2015) ou les deux (Thompson *et al.*, 2017 ; Warkentin *et al.*, 2016).

Les types de comportements étudiés correspondent à des comportements génériques comme « la mise en place de mesures de sécurité » (Workman *et al.*, 2008) ou à des comportements plus précis qui vont de l'utilisation d'antivirus (Gurung *et al.*, 2009 ; Hanus et Wu, 2016) à la

mise à jour de firewalls (Hanus et Wu, 2016), en passant par le changement de mots de passe (Johnston *et al.*, 2015).

### *1.2.4. Publications et travaux basés sur la PMT*

Après une communication dans la conférence de l'AIM en 2015, nous avons publié un article dans SIM en 2017 (SIM, 2017). Cette recherche reflète trois grands changements stratégiques. Premièrement l'écriture à plusieurs auteurs, puisqu'il a été co-écrit avec Katherine Gundolf et Annabelle Jaouen, deuxièmement il représente un passage à la langue anglaise et troisièmement une orientation vers des études plus quantitatives.

Le fait de travailler à plusieurs m'a permis d'étendre le spectre des publications possibles en croisant les divers cadres théoriques voire les disciplines de gestion. Nous verrons par la suite les enrichissements apportés en croisant S.I. et entrepreneuriat, S.I. et stratégie ou encore S.I. et innovation. De la même manière, travailler à plusieurs est une source d'opportunités de publications, notamment en profitant des compétences de chacun et en partageant des idées.

La langue anglaise a été adoptée dans le but d'augmenter la visibilité de mes travaux et de viser à terme des revues internationales, si possible de rang 1 CNRS/FNEGE.

Le passage aux études quantitatives a permis de valider certaines hypothèses sur des échantillons de grande taille (200 à 340 répondants). Un aspect plus pratique de ce choix tient aux aides accordées par mon institution. S'il m'est possible d'avoir accès à des financements pour s'assurer de la soumission de questionnaires quantitatifs à des panels, il m'est quasiment impossible d'avoir des aides pour les retranscriptions d'entretiens qualitatifs. J'ai choisi de me spécialiser dans les équations structurelles en moindres carrés partiels (Partial Least Squares Structural Equation Modelling, ou PLS-SEM) car ce type d'analyses présente de nombreuses qualités, parmi lesquelles l'aptitude à manipuler des modèles complexes, à inclure des construits de type réflectif ET formatif, et à traiter des variables modératrices et hiérarchiques (Hair *et al.*, 2011 ; Hair *et al.*, 2019 ; Sarstedt *et al.*, 2014). Cependant, cela a nécessité une auto-formation et des formations à plusieurs méthodes d'analyse de données. J'ai eu la chance de bénéficier des enseignements de professeurs renommés dans le domaine des statistiques comme Pierre Valette-Florence ou bien très impliqués dans des logiciels reconnus comme SmartPLS (Christian Ringle et Marko Sarstedt) et Adanco (Jorg Henseler).

Cet article s'intitule « *CEOs' Information Security Behavior in SMEs: Does Ownership Matter?* » et a été publié dans Systèmes d'Information et Management, volume 22, n°3, p. 7-45. Il traite de la question de recherche suivante : *« Quels facteurs peuvent expliquer les comportements relatifs à la protection des informations des dirigeants de PME ?* »

Pour cette étude empirique qualitative, nous avons mobilisé la 'core' PMT, que nous avons enrichie avec l'influence sociale, en conformité avec nos travaux précédents. Au sujet de l'influence sociale, des études sur les PME ont montré que les dirigeants se basent souvent sur leurs réseaux sociaux et professionnels pour prendre des décisions, et de telles influences sociales peuvent constituer une variable pertinente pour expliquer les comportements des dirigeants (Ozgen et Baron, 2007 ; Schoonjans *et al.*, 2013). L'influence sociale (Ajzen, 1991) peut être considérée comme équivalente aux normes subjectives (voir Venkatesh *et al.*, 2003), dans la mesure où elle fait référence à la « *pression sociale perçue exercée par des personnes importantes pour quelqu'un. Cela correspond à la perception d'un individu que la plupart des personnes importantes pour lui pensent qu'il devrait ou non adopter le comportement en question* » (Fishbein et Ajzen, 1975, p. 302).

En conséquence, le modèle utilisé est représenté ci-dessous en figure 7.

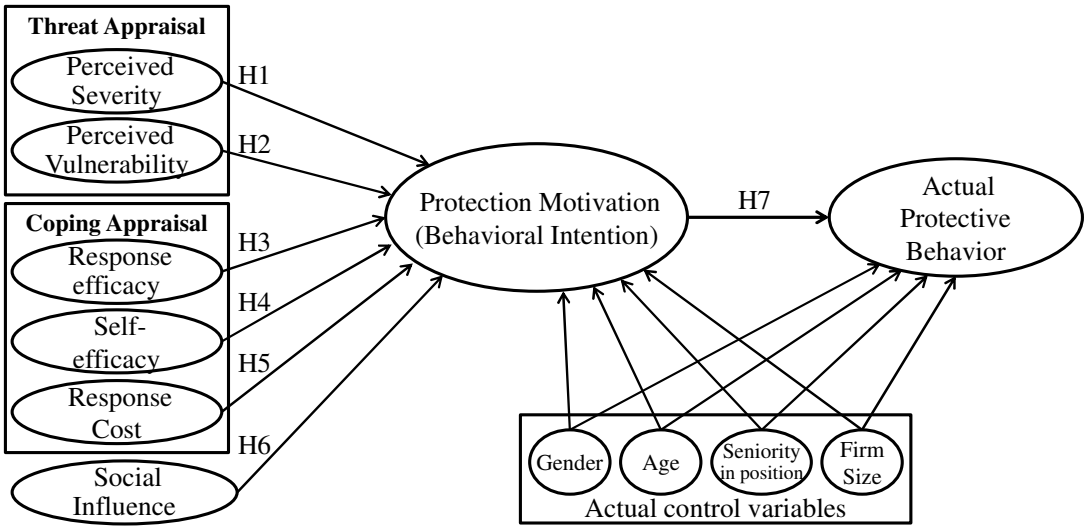


**Figure 7. Modèle utilisé dans l'article SIM (2017)**

Nous avons mené une étude auprès de 292 dirigeants de PME, les données collectées ont été analysées par la méthode des moindres carrés partiels (PLS) en utilisant des équations structurelles (SEM). La littérature académique ayant montré que le comportement des dirigeants de PME était influencé par le fait d'être ou non propriétaires de leur entreprise, nous avons testé le pouvoir explicatif de la PMT sur les deux sous-populations : les dirigeants propriétaires (n=183) et non-propriétaires (n=109). Nos résultats mettent en évidence des différences très importantes et significatives entre ces deux sous-groupes.

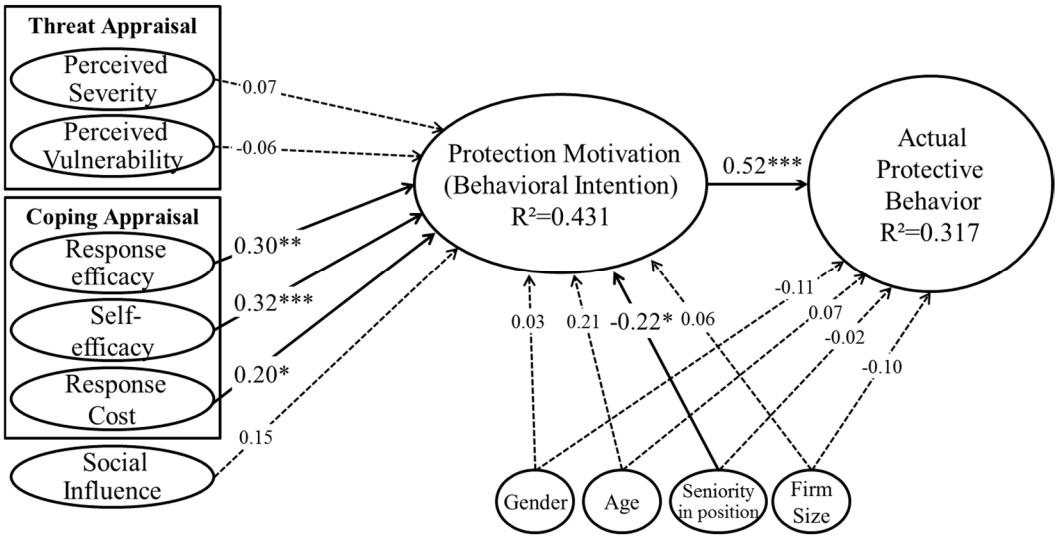


**Figure 8. Résultats pour les dirigeants non-propriétaires (n=109)**

En figure 8, le comportement des dirigeants non-propriétaires est conforme aux résultats des études antérieures sur la core PMT. L'évaluation du comportement de 'coping' est la principale raison qui incite les dirigeants non-propriétaires à mettre en œuvre des mesures de sécurité de l'information, tandis que l'évaluation de la menace et l'influence sociale ont des effets bien moins importants. À l'inverse, les dirigeants propriétaires ont des comportements très différents, comme le montre la figure 9.

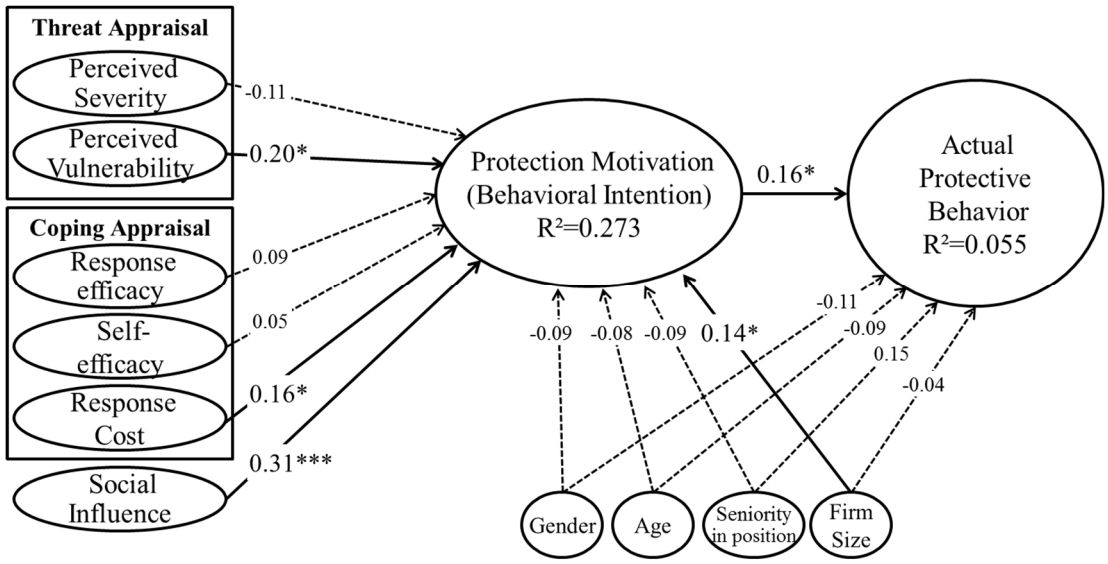


**Figure 9. Résultats pour les dirigeants propriétaires (n=183)**

Les contributions théoriques de notre travail sont les suivantes. Tout d'abord, il s'agissait de la première étude qui se focalisait uniquement sur la motivation à la protection des dirigeants de PME. De plus, nous n'avons trouvé aucune étude académique analysant les comportements en SSI (voire même en SI) basée sur le fait que le dirigeant soit propriétaire ou non de son entreprise. Alors que nos résultats pour les dirigeants non-propriétaires confirment et étendent les recherches antérieures sur la PMT, les comportements des dirigeants propriétaires présentent des spécificités importantes. Pour expliquer ceci, nous avons proposé des théories qui complètent la PMT, telles que la théorie de l'agence. Nous avons aussi montré que l'influence sociale était un construit très important pour expliquer les comportements des dirigeants propriétaires de leur entreprise.

Nos contributions managériales découlent de l'importance de l'influence sociale, de ce fait les experts professionnels, tels que les experts-comptables (AIM, 2011), les institutions et toutes les structures d'appui faisant partie de l'écosystème des PME, doivent être conscients de leur rôle de conseillers. Ils pourraient aider les propriétaires à agir, ou au moins à mieux prendre conscience de l'importance de la protection des informations. Mais surtout, comme les facteurs qui sont à la base des comportements de protection des dirigeants-propriétaires sont presque en contraste total comparés à ceux des dirigeants non-propriétaires, toute communication ou action devrait être spécifiquement adaptée à chacune de ces deux populations. Par exemple, en se référant aux figures 8 et 9, la motivation à la protection des dirigeants *non-propriétaires* pourrait être améliorée en développant leur niveau d'efficacité personnelle relative à la SSI et leur confiance dans l'efficacité des solutions à mettre en place. Pour les dirigeants *propriétaires*, ce serait plutôt l'influence de leurs pairs ou de leur réseau professionnel qui les motiverait à agir pour une meilleure protection de leurs informations.

Notre article mettait en évidence plusieurs pistes de recherches parmi lesquelles nous en avons retenues deux : premièrement, la nécessité d'une étude qualitative approfondie afin d'identifier d'autres variables pertinentes pour mieux prendre en compte l'écart très spécifique entre dirigeants propriétaires et non-propriétaires. Deuxièmement, l'intérêt de mieux prendre en compte le partage des rôles entre les acteurs (dirigeants, DSI, entreprises de services) et d'inclure la notion de comportement direct (faire) et indirect (soutenir la personne qui fait) lorsque le dirigeant n'agit pas.

### *1.2.5. Conclusion : vers des enrichissements de la PMT*

Nous avons vu plus haut que la PMT (Rogers, 1983) est l'une des théories de référence pour étudier les comportements relatifs à la sécurité de l'information. Toutefois, elle souffre de certaines limitations.

Après notre publication dans SIM (2017), nous avons décidé de nous recentrer sur la forme la plus simple de la PMT, c'est-à-dire la 'core' PMT sans le construit 'response cost' car (1) il n'est pas toujours utilisé et quand il est utilisé, il est soit (2) non-significatif, soit (3) son effet est contraire à l'hypothèse. Au total, sur 37 études sur la PMT, le 'response cost' n'a eu l'effet escompté que dans 32% des cas, soit moins du tiers des études (voir Annexe 2).

Mais la plus importante limitation de la PMT est double. Premièrement, elle n'est basée en amont uniquement que sur des événements menaçants, alors que la théorie du coping de Lazarus prend aussi en compte d'éventuelles opportunités. Pourtant, dans leur article de 2005, Beaudry et Pinsonneault ont montré que dans le domaine des S.I. un évènement relatif aux technologies de l'information peut être considéré comme une menace et/ou une opportunité.

Deuxièmement, la PMT n'explique en aval que des comportements centrés-problème et ne prend donc pas en compte les comportements centrés-émotion, pourtant inclus dans la théorie originelle du coping de Lazarus (1966). Or, les stratégies comportementales qui découlent de l'appréciation primaire de l'introduction de technologies radicales en S.I., peuvent être centrées-problème mais aussi centrées-émotion. Pourtant, la PMT vise uniquement à expliquer la motivation (ou non, voir Workman *et al.*, 2008) à mettre en place des mesures de sécurité au sens large (Moody *et al.*, 2018). Mais, même en sécurité de l'information, ce n'est pas parce qu'un individu n'adopte pas une stratégie de coping centrée-problème qu'il ne va pas opter pour des stratégies plus centrées-émotion : par exemple, la PMT arrivera à expliquer certaines mesures mises en place (centrées-problème) par un acteur pour contrer une menace, mais on ne pourra pas identifier l'état émotionnel ou cognitif d'un individu (caractérisé par ses stratégies centrées-émotion) s'il n'a pas mis en place ces mesures. En effet, un individu pourra entrer dans des comportements de réappréciation positive de l'évènement, de distanciation, de déni, d'évitement, etc. (Carver *et al.*, 1989 ; Lazarus et Folkman, 1984 ; Folkman et Lazarus, 1988). Enfin, une menace pourra aussi découler de la saisie d'une opportunité relative à l'introduction d'une nouvelle technologie.

D'où la nécessité d'examiner de nouvelles approches pour dépasser ces limitations.

## 1.3. Coping model of user adaptation (CMUA) et transformations radicales

Les technologies numériques (digital technologies) correspondent aux médias sociaux, à la mobilité, au big data et au cloud computing (Sultan , 2013) et constituent « *le moteur des transformations en entreprise* », selon le Cigref (2013). En effet, les technologies numériques « *transforment fondamentalement les stratégies d'entreprises, les processus métiers, les capacités des entreprises, les produits et services et les relations-clé interentreprises dans des réseaux d'affaires étendus* » (Bharadwaj *et al.*, 2013, p. 471). Ces technologies et les changements radicaux induits (Karimi et Walter, 2015) vont donc générer des risques pour les organisations (Venkatraman, 1991 ; Xue *et al.*, 2013), mais aussi vont déclencher de nouveaux usages qui, à leur tour, vont générer de nouvelles problématiques de sécurité.

C'est pourquoi je me suis intéressé à plusieurs de ces technologies numériques (colloque MTO, 2014), telles que l'informatique en nuage ou 'cloud computing' (revue MTO, 2015), les médias sociaux (revue MTO, 2013), ainsi qu'au big data (colloque MTO, 2015).

Si j'ai examiné les opportunités offertes par ces technologies, je me suis aussi intéressé aux menaces qu'elles peuvent poser en termes de sécurité de l'information, que ce soit pour les

informations de l'entreprise elle-même (vision des dirigeants), mais aussi pour les informations personnelles (vision des employés), dans le cadre notamment de la protection des informations relatives à la vie privée.

### *1.3.1. Transformations radicales : opportunités et menaces relatives au BYOD*

Dans ce contexte, nous avons étudié le phénomène du BYOD ou 'bring your own device' qui consiste en l'utilisation par les salariés de leurs outils personnels dans un contexte professionnel, que ce soient des ordinateurs portables, des tablettes ou des téléphones mobiles, et en particulier des smartphones. Ces utilisations sur le lieu de travail peuvent se faire à des fins personnelles (par exemple, pour rester en contact avec ses proches) ou à des fins professionnelles (Singh, 2012 ; Weeger *et al.*, 2016).

Le BYOD présente un double intérêt, dans la mesure où non seulement il facilite la mobilité et la communication en entreprise, mais aussi parce qu'il représente un exemple de 'consumérisation' des technologies de l'information. La consumérisation des T.I. se traduit par l'adoption, dans un contexte de travail, de technologies du marché grand public (Ortbach *et al.*, 2013 ; De Kok *et al.*, 2015 ; Mueller *et al.*, 2016). Nous verrons par la suite que la consumérisation peut aboutir à un phénomène original d'adoption inversée des technologies. Cette optique d'adoption inversée reflète, là encore, notre philosophie d'étudier des comportements 'libres', c'est-à-dire non imposés par la direction, comme c'est souvent le cas dans le cadre d'une adoption classique.

Cette adoption par les salariés du BYOD montre que cette manière de travailler présente des opportunités pour eux-mêmes (Yun *et al.*, 2012 ; Kim *et al.*, 2013 ; Marshall, 2014 ; Whitten *et al.*, 2014). Mais le fait que les dirigeants d'entreprise puissent autoriser cet usage des outils mobiles de leurs salariés reflète qu'ils perçoivent aussi le BYOD comme une opportunité. Le revers de la médaille est que l'implémentation du BYOD en entreprise va entrainer des dangers, que ce soit pour les données personnelles des salariés, mais aussi pour les données de l'entreprise, et donc représenter une menace pour les dirigeants de ces entreprises. Certains de ces dangers sont d'ailleurs directement la conséquence de cette adoption inversée et de la propriété de l'outil mobile (Hovav et Putri, 2016).

Nous allons maintenant présenter nos travaux qui ont permis (1) de compléter la définition de la *logique d'adoption inversée* ou 'reversed adoption logic' à partir des travaux de Leclercq-Vandelannoitte (2015a, 2015b), (2) de montrer que le BYOD s'avère source d'innovations managériales avec des effets *facilitateurs* et *induits*, (3) d'étudier plus précisément les impacts du BYOD en milieu hospitalier, et (4) de définir la notion de (double) *paradoxe de sécurité* et de préparer des travaux sur ces paradoxes.

### *1.3.2. Publications et travaux : du BYOD au CMUA*

Nos travaux dans le cadre du BYOD ont donné lieu dans un premier temps à deux participations dans des colloques (Pré-ICIS, 2016 ; AIM, 2017), ainsi qu'à trois articles conceptuels publiés en 2018 dans Politiques et Management Public, Journal of Organizational Change Management et International Journal of Information Management. Ces trois articles ont été co-écrits avec Paméla Baillette (université de Perpignan[5]), ils posent les bases de nos travaux ultérieurs qui vont utiliser le CMUA dans le cadre d'études quantitatives.

[5] Elle occupe le poste de maître de conférences à l'IAE de Bordeaux fin 2018.

*1.3.2.1. L'article JOCM, 2018*

Le premier article a pour titre « *BYOD-related innovations and organizational change for entrepreneurs and their employees in SMEs: the identification of a twofold security paradox* » et a été publié dans le Journal of Organizational Change Management, volume 31, n°4, p. 839-851. Cet article vise à répondre aux questions de recherche suivantes : Quels sont les avantages et les dangers des pratiques liées au BYOD pour les entrepreneurs et leurs employés ? Enfin, quels paradoxes peuvent apparaître en termes de sécurité de l'information ?

Dans une première partie, nous montrons tout d'abord que le BYOD va constituer une source d'innovations technologiques grâce à l'introduction de nouvelles applications mobiles, et va aussi dans une certaine mesure réduire les coûts pour les organisations, puisque les coûts d'achats des outils informatiques sont en partie 'délégués' auprès des salariés. Deuxièmement, le BYOD va déclencher l'adoption de nouvelles pratiques organisationnelles découlant d'une plus grande liberté d'utilisation, d'une flexibilité améliorée et d'une réactivité plus importante. Le BYOD va aussi rendre réduire la frontière entre la vie professionnelle et la vie privée du salarié, ce qui dans un certain sens présente des avantages, comme une proximité conservée avec ses proches, mais va aussi introduire des risques accrus, notamment pour les informations ayant trait à la vie privée du salarié et les informations manipulées par l'organisation.

La seconde partie de l'article met en évidence les risques posés par le BYOD. Pour les salariés, une utilisation accrue va augmenter la probabilité de casse ou de vol de l'outil. De plus, une politique de sécurisation des outils mobiles ou mobile device management (MDM) peut exister dans l'entreprise. Si ce MDM est trop durement paramétré, une erreur du salarié ou la détection d'un simple virus peut provoquer le blocage complet de l'appareil qui devient alors une 'brique' inutilisable ou bien provoquer l'effacement des données stockées dans l'appareil, pouvant inclure les données personnelles. Pour les organisations, le BYOD peut devenir la source de nouvelles vulnérabilités ou de failles de sécurité. Premièrement, un smartphone est une cible de choix pour les cybercriminels, car contrairement aux ordinateurs portables, les antivirus et firewalls sont bien moins fréquemment installés sur les téléphones mobiles. De plus, un salarié aura des comportements plus risqués sur son outil personnel (Hovav et Putri, 2016). Enfin, du fait de sa connectivité accrue, un smartphone aura accès non seulement aux réseaux mobiles (2G à 5G) mais aussi au bluetooth et au wifi, ouvrant ainsi des failles sur ces divers réseaux.

Cet article conclut sur la création de paradoxes de sécurité, à la fois pour les dirigeants et les salariés et propose une définition pour chacun de ces deux paradoxes de sécurité. D'un côté, les salariés, sont partagés entre leur désir de protéger l'utilisation, le stockage et la diffusion de leurs données personnelles et leur désir de profiter des avantages procurés par les innovations technologiques dans leur vie personnelle et sociale (Pras, 2012). Un paradoxe 'confidentialité / personnalisation' a déjà été identifié (Sheng *et al.*, 2008). Cette intrusion perçue dans la vie privée peut être compensée par certains avantages, notamment l'authentification rapide, la publicité ciblée, l'utilité et la facilité d'utilisation (Keith *et al.*, 2013 ; Sutanto *et al.*, 2013). Ces avantages perçus sont jugés suffisamment positifs pour compenser les facteurs dissuasifs associés au risque de divulgation des informations personnelles. Dans l'article AIM de 2017, Baillette et Barlette définissent la préoccupation au sujet des données personnelles comme « *la tendance générale d'un individu à s'inquiéter de la sécurité de leurs informations personnelles* ». Pourtant, si les utilisateurs ne souhaitent pas divulguer leurs informations personnelles, ils les mettent néanmoins en danger. Par conséquent, pour les utilisateurs d'outil BYOD, le concept de '*paradoxe de sécurité*' peut être défini comme suit : « *lorsque la perception des avantages du BYOD dépasse celle des risques encourus, les utilisateurs peuvent mettre en danger leurs données personnelles par le biais de leurs pratiques relatives au BYOD sans mettre en œuvre une protection suffisante, malgré une affirmation forte de leurs préoccupations concernant la sécurité de leurs données personnelles* ».

D'un autre côté les dirigeants d'entreprise adoptent des processus cognitifs spécifiques, dans un environnement caractérisé par la nécessité de performances (Messeghem et Torrès, 2015 ; Schmitt, 2015). En référence à la théorie de la 'catégorisation', Palich et Bagby (1995) ont montré que les décisions entrepreneuriales peuvent être étudiées en tant que processus cognitifs, en mettant l'accent sur des biais heuristiques et cognitifs. Les entrepreneurs ont tendance à 'catégoriser' les situations en percevant plus d'opportunités que de menaces et plus de forces que de faiblesses. Cette approche reflète une tendance à percevoir les situations de manière positive (Palich et Bagby, 1995 ; Fayolle *et al.*, 2008). Les entrepreneurs font des compromis entre le risque d'échec ('couler le navire'), correspondant aux pertes potentielles et leur évaluation des pertes acceptables, et le risque de manquer une occasion ('rater le navire'), faisant référence aux gains potentiels. Fayolle *et al.* (2008) évoquent la 'vision positive du monde' des entrepreneurs, telle que mise en évidence par Palich et Bagby (1995) : les biais cognitifs et les heuristiques tels que la sur-confiance ou la catégorisation sont tous liés à une forme d'optimisme excessif et sont plus courants chez les entrepreneurs (Fayolle *et al.*, 2008). Cette vision peut s'avérer préjudiciable dans le contexte du BYOD, qui crée des risques pour la sécurité des informations de leur entreprise, qu'elles soient stockées dans les bases de données ou les outils BYOD des employés. En effet, les entrepreneurs reconnaissent les avantages apportés par le BYOD, mais ne sont pas conscients du risque réel que représentent les technologies et les pratiques liées au BYOD, mettant ainsi potentiellement en danger leurs activités. D'une part, l'entrepreneur considère les avantages pour l'entreprise (c'est-à-dire plus d'efficience et de flexibilité) et une satisfaction accrue de ses employés ; D'autre part, le niveau de risque auquel l'entreprise est confrontée augmente considérablement. Par conséquent, l'entrepreneur va réaliser un 'calcul de sécurité de l'information' dans lequel les avantages supplémentaires sont plus ou moins bien équilibrés par les risques supplémentaires. Pour les organisations, le concept de '*paradoxe de sécurité*' dans le contexte du BYOD peut être défini comme suit : « *Lorsque la perception des avantages du BYOD l'emporte sur les risques, les dirigeants d'entreprises peuvent mettre en danger leurs données en autorisant ou en encourageant les utilisateurs à travailler en mode BYOD sans implémenter de mesures de sécurité suffisantes, malgré une affirmation forte de leurs préoccupations concernant la sécurité des informations de leur entreprise ».*

Les principaux apports de ce travail sont la mise en évidence et la définition de ces deux paradoxes de sécurité, pour les dirigeants et les salariés.

#### *1.3.2.2. L'article P&MP, 2018*

Le deuxième article a pour titre « *BYOD et innovations managériales en contexte hospitalier : mise en évidence d'une logique d'adoption inversée* » et a été publié dans Politiques et Management Public, volume 35, n°1, p. 49-68.

Cet article se base sur l'exemple de l'utilisation des outils mobiles personnels en contexte hospitalier pour montrer comment le BYOD, en tant que mise en place d'une innovation technologique, peut générer des innovations managériales. Il vise à répondre à la question de recherche suivante : « *Dans quelle mesure l'appréhension des risques et des opportunités du BYOD en contexte hospitalier peut-elle s'avérer source d'innovations managériales ?* ». Selon Birkinshaw et Mol (2006) l'innovation managériale relève de pratiques, de techniques de management ou de processus nouveaux, qui sont significativement différents des normes habituelles. Exprimé simplement, *« l'innovation managériale change la façon dont les managers font ce qu'ils font*[6] » (Hamel, 2006, p. 3).

[6] "*Put simply, management innovation changes how managers do what they do*" (Hamel, 2006, p. 3).

Dans cet article, nous montrons que le BYOD s'avère source d'innovations managériales, à la fois *facilitées* par les nouvelles pratiques que permet le BYOD, mais aussi *induites* par la mise en place de solutions adaptées aux nouveaux risques inhérents au fonctionnement en mode BYOD.

Nous avons choisi le contexte hospitalier car les hôpitaux sont actuellement soumis à de profondes mutations induites par des exigences de rentabilité (Bérard *et al.*, 2015 ; Bourret *et al.*, 2013) qui les contraignent à innover (Djellal, 2014), en transformant leurs pratiques managériales au-delà de l'innovation thérapeutique ou technologique (Nobre, 2013). Dans ce contexte, nous présentons trois exemples d'innovations managériales qui ont été *facilitées* par l'introduction du BYOD dans les hôpitaux (Harris *et al.*, 2012 ; Marshall, 2014 ; Motulsky *et al.*, 2017). Nous analysons dans un second temps les risques posés par le BYOD, qui sont d'autant plus importants qu'ils portent particulièrement sur les données concernant les patients, considérées comme sensibles. Ces données sont protégées par le Code de la santé publique. Pourtant, des fuites de données se manifestent parfois en provenance de centres hospitaliers français, notamment via l'accès par internet à des données confidentielles[7]. Par exemple, la CNIL a mis en demeure en 2013[8] un centre hospitalier qui avait accordé l'accès à l'un de ses prestataires informatiques aux dossiers médicaux de plusieurs centaines de patients, en méconnaissance des dispositions du Code de la santé publique et de la loi informatique et libertés relatives au respect de la vie privée des patients ainsi qu'à la sécurité de leurs données médicales. A la suite de l'intervention de la CNIL, ce centre hospitalier s'est remis en conformité.

Nous défendons ensuite le fait que toutes ces mesures de sécurité à mettre en place pour compenser celles qui ont été générées par l'introduction du BYOD entrainent des changements de pratiques qui sont donc en conséquence des innovations managériales *induites*. Nous terminons par une synthèse de notre recherche théorique par une schématisation en figure 10 de ces innovations managériales *facilitées* et *induites* par le BYOD.

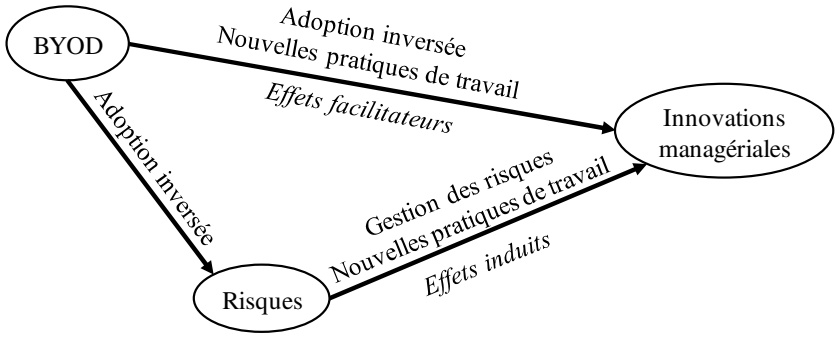


**Figure 10. Les effets du BYOD sur les innovations managériales**

Le principal apport théorique de cette recherche est cette conceptualisation des effets du BYOD, tout particulièrement en milieu hospitalier. Sur le plan managérial, notre article permet de sensibiliser les décideurs en milieu hospitalier, à la fois sur les apports potentiels du BYOD, mais aussi sur les risques spécifiques qui en découlent, et propose des exemples ainsi que des

[7] http://www.huffingtonpost.fr/barbara-bertholet/donnees-medicales-en-ligne_b_3162327.html

[8] Délibération CNIL n°2013-037 du 25 septembre 2013 mettant en demeure le centre hospitalier de Saint-Malo, et Communiqué CNIL intitulé "*Clôture de la mise en demeure adoptée à l'encontre du centre hospitalier de Saint-Malo*" du 17 octobre 2013.

solutions pour en maximiser les apports tout en en diminuant les risques, a fortiori dans un contexte particulièrement sensible.

*1.3.2.3. L'article IJIM, 2018*

Le troisième article a pour titre « *Bring Your Own Device in organizations: Extending the reversed IT adoption logic to security paradoxes for CEOs and end-users* » et a été publié dans International Journal of Information Management, volume 43, p. 76-84. Pour ce travail, nous avons fait appel à Aurélie Leclercq-Vandelannoitte qui avait posé les bases de l'adoption inversée des T.I. dans ses travaux, ce qui non seulement a permis d'enrichir nos réflexions communes, mais de créer des relations favorables pour de futures collaborations.

Cet article traite d'une question de recherche multiple : « *Quels sont les avantages et les risques pour les dirigeants et les utilisateurs finaux de la logique d'adoption inversée du BYOD et comment peut-on surmonter les paradoxes de sécurité relatifs à l'introduction du BYOD en organisation ?* »

Ce travail propose une version plus aboutie de l'introduction du BYOD en entreprise vue en tant que manifestation d'un phénomène d'adoption inversée. Nous mettons ainsi, dans une première partie, en regard l'adoption traditionnelle face à l'adoption inversée, ce qui nous permet de montrer que l'on passe d'une trajectoire *top-down* (adoption traditionnelle) à une nouvelle trajectoire *bottom-up* (dite d'adoption inversée), illustrée dans la figure 11.

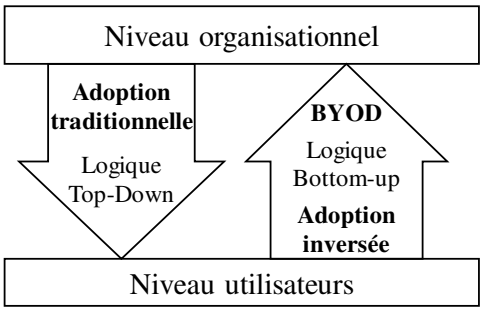


**Figure 11. Le BYOD : d'une adoption traditionnelle à une adoption inversée**
(inspiré des travaux de Leclercq-Vandelannoitte 2015a, 2015b)

Nous examinons ensuite les avantages et les risques posés par cette adoption inversée en introduisant notamment le concept de 'génération' (faisant référence aux générations X, Y, et Z) qui sera repris dans l'un de nos projets à venir. Sur la partie des risques, après avoir repris nos travaux précédents sur les paradoxes de sécurité, nous proposons de nombreux exemples de solutions pour aller au-delà de ces paradoxes et limiter leur apparition.

Nos deux principales contributions théoriques sont cet approfondissement des notions d'adoption inversée et des situations à l'origine de paradoxes de sécurité. Nos contributions managériales résident dans les conseils donnés, qui portent de manière systématique sur la maximisation des avantages relatifs à l'introduction du BYOD, mais aussi sur la minimisation des risques.

Ces trois articles, qui présentent des visions complémentaires des opportunités et des menaces présentées par le BYOD, ont préparé les fondements de plusieurs études quantitatives menées auprès de salariés et de dirigeants. Ces études nous ont permis d'écrire plusieurs articles dont certains sont déjà acceptés (JGIM, 2020) ou en révision (IJIM, R3) et d'autres sont en cours d'écriture à ce jour. A cet effet, nous avons utilisé comme modèle de recherche le *coping model of user adaptation* (CMUA), toujours basé sur les théories du coping. Ce modèle prend en compte les opportunités et les risques associés à l'introduction d'une technologie pouvant

provoquer un changement radical (disruptive technology) en entreprise (Beaudry et Pinsonneault, 2005, 2010).

### *1.3.3. Le CMUA et ses apports*

Le CMUA (coping model of user adaptation) est, lui aussi, basé sur la théorie du 'coping' de Lazarus (1966). Il contient les deux processus d'appréciation primaire et secondaire déjà étudiés dans le paragraphe 1.1.5.

Le processus primaire correspond à une appréciation de l'évènement, correspondant à l'introduction d'une technologie de l'information 'disruptive', perçue comme une opportunité et/ou une menace. Il est suivi par une appréciation du comportement de 'coping' à exercer, qui va entrainer des efforts d'adaptation. Ces efforts vont conduire l'individu à opter pour diverses stratégies de coping (voir figure 12).

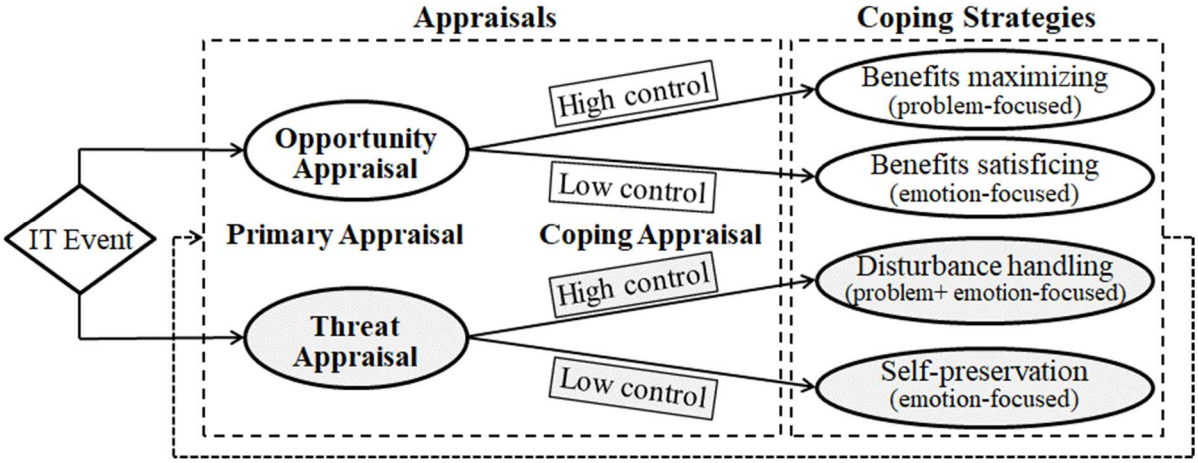


**Figure 12. Le CMUA. Adapté de Beaudry et Pinsonneault (2005).**

#### *1.3.3.1. Appréciation primaire relative aux T.I.*

Le processus de coping d'un individu commence lorsqu'un utilisateur prend conscience des conséquences potentielles d'un événement informatique important et évalue sa pertinence et son importance personnelles et/ou professionnelles (Folkman, 1992 ; Beaudry et Pinsonneault, 2005). Par exemple, un individu peut penser qu'un nouvel outil (matériel ou logiciel) lui permettra d'améliorer son efficience ou ses capacités d'échanges avec les autres, il pourra donc intégrer ce nouveau matériel ou logiciel dans ses routines de travail, ce qui pourra nécessiter une (auto)formation à l'usage de ce nouvel outil. A l'inverse, ce nouvel outil apparaîtra comme une menace pour l'individu, s'il se sent insuffisamment compétent pour l'utiliser ou si son utilisation peut mettre en danger sa vie privée. La plupart des événements informatiques ont plusieurs facettes et un individu pourra les considérer comme des menaces, des opportunités ou bien les deux (Beaudry et Pinsonneault, 2005). Dans le dernier cas, ce sera leur importance relative qui aura une influence sur le choix des efforts d'adaptation à réaliser (Lazarus et Folkman, 1984). Il est à noter que la théorie du coping initiale de Lazarus ne donne pas d'indication sur l'appréciation primaire car elle est "*muette quant aux éléments d'une disruption utilisés dans l'appréciation primaire*"[9] (Beaudry et Pinsonneault, 2005, p. 498). Nous verrons ultérieurement comment compléter le modèle théorique pour faciliter cette appréciation primaire.

[9] "*mute regarding what elements of a disruption are used in primary appraisal*".

Certains éléments pourront influencer cette évaluation, comme le fait que l'outil soit perçu comme concret ou que les résultats obtenus aient un impact critique. De même, le niveau de 'task-technology fit' ou de performance espérée pourra donner lieu une perception négative (s'il est faible) ou positive (s'il est fort). Certains facteurs sociaux ou institutionnels peuvent entrer en jeu, tels que l'opinion des pairs ou de la hiérarchie à propos de l'outil (Taylor et Todd 1995 ; Venkatesh *et al.*, 2003). Le top management support (TMS) peut aussi avoir une influence positive sur la perception des individus. Enfin, il a été montré que les normes institutionnelles et subjectives associées à l'acceptation et à l'utilisation de la technologie peuvent influencer l'appréciation primaire (DiMaggio et Powell, 1983 ; Venkatesh *et al.*, 2003).

L'appréciation primaire des menaces et des opportunités va conduire à une appréciation secondaire, le 'coping appraisal', qui correspond à l'appréciation par l'individu de sa capacité à gérer cette menace et/ou à éviter une situation qui est source de menaces ou de sa capacité à saisir et/ou bénéficier d'une situation qui est source d'opportunités.

#### *1.3.3.2. Appréciation secondaire – maîtrise perçue du comportement*

L'appréciation secondaire (ou *coping appraisal)* est l'évaluation des options disponibles qui va guider le choix de *stratégies* de *coping* par l'individu*,* qu'elles soient centrées-*problème* ou centrées-*émotion*, dépendant du niveau de maîtrise de la situation perçu par l'individu.

Pour Beaudry et Pinsonneault (2005), trois composantes principales vont former l'appréciation secondaire par l'individu : la maîtrise des conditions de travail (autonomie), la maîtrise personnelle, et enfin la maîtrise de la technologie. La *maîtrise des conditions de travail* correspond au degré d'autonomie dont dispose l'utilisateur pour modifier ses tâches en réponse à un événement informatique. La *maîtrise personnelle* correspond à la capacité perçue par l'individu à s'adapter au nouvel environnement (Lazarus et Folkman, 1984). Enfin, la *maîtrise de la technologie* désigne l'influence que les utilisateurs ont sur les caractéristiques et les fonctionnalités du matériel/logiciel.

Les appréciations primaire et secondaire vont conduire à des stratégies de coping 'centrées-émotion' et 'centrées-problème' (Beaudry et Pinsonneault, 2005 ; Lazarus et Folkman, 1984). Conformément à la théorie du coping, Beaudry et Pinsonneault (2005) ont postulé qu'un fort niveau de maîtrise conduisait principalement à des stratégies de coping 'centrées-problème', alors qu'un faible niveau de maîtrise conduisait à des stratégies 'centrées-émotion'.

#### *1.3.3.3. Les stratégies de coping relatives aux T.I.*

Le CMUA postule que face à un événement, quatre stratégies de coping (cf. tableau 4) peuvent être adoptées, dépendant d'une part de la perception par l'individu de l'évènement en tant qu'opportunité ou menace, et d'autre part du niveau de maîtrise perçue par l'individu du comportement à adopter (Beaudry et Pinsonneault, 2005, 2010 ; Moser *et al.*, 2011).

| Control<br>Appraisal | Low<br>(emotion-focused) | High<br>(mainly problem-focused) |
|---|---|---|
| Opportunity | Benefits Satisficing | Benefits Maximizing |
| Threat | Self-Preservation | Disturbance Handling[10] |

**Tableau 4. Les quatre stratégies de coping**
(adapté de Beaudry et Pinsonneault, 2005)

[10] Certains comportements centrés-émotion peuvent aussi se produire, dans une moindre mesure (cf. tableau 5).

La stratégie ‘profiter des avantages’ (*benefits satisficing*) correspond à l’exercice d’un minimum d'efforts centrés-problème pour deux raisons : premièrement, la situation étant perçue comme étant bénéfique, il n'y a pas un réel besoin d'agir ; deuxièmement, la maîtrise perçue étant faible, la réaction sera principalement centrée-émotion. De plus, aucune tension émotionnelle n’émanant de l'événement, il n'est pas nécessaire de réduire une quelconque tension. Par conséquent, un individu restera plutôt passif si un évènement est perçu comme bénéfique et qu’il n’a pas de maîtrise sur celui-ci.

La stratégie ‘maximiser les avantages’ (*benefits maximizing*) est adoptée quand un individu perçoit un événement relatif aux T.I. comme une opportunité et que sa maîtrise perçue de la situation est élevée. Dans un tel cas, cette stratégie de coping centrée-problème vise à maximiser les avantages personnels ou professionnels offerts par l'événement T.I. Par exemple, un individu peut modifier ses conditions de travail (un logiciel pourra soulager un individu des tâches répétitives et basiques et permettra son recentrage sur des tâches plus stratégiques), la technologie (personnaliser le logiciel ou ses fonctionnalités), ou son cadre personnel (se former, adapter son comportement à la suite de l’introduction de la T.I.). Globalement, ces efforts d’adaptation pourront améliorer les performances des individus (réduction des erreurs, efficience du travail, etc.).

Dans le cas d’une situation potentiellement menaçante, un niveau élevé de maîtrise perçue sur le comportement de coping conduira à la stratégie ‘gérer la perturbation’ (*disturbance handling*), principalement centrée-problème. Les efforts des individus auront pour but d’éviter la survenance ou de minimiser les conséquences de cet évènement négatif. Les efforts d’adaptation pourront concerner les conditions de travail (intégrer des pratiques de sécurité dans son travail), la technologie (faire des sauvegardes, lancer un antivirus), ou l’individu lui-même (se former). Une stratégie centrée-émotion (voir ‘préservation de soi’ ci-dessous) pourra être adoptée en complément afin de restaurer la stabilité émotionnelle (Folkman 1992 ; Folkman *et al.*, 1986).

Un niveau faible de maîtrise perçue du comportement conduira à l’adoption d’une stratégie de coping plus passive et donc centrée-émotion, la ‘préservation de soi’ (*self-preservation*). Cette stratégie peut restaurer un équilibre émotionnel, mais n’aura que peu voire pas d’impact sur la performance de l’individu. Cette stratégie de réduction des tensions qui émanent de l’évènement va conduire à des adaptations diverses afin de minimiser les conséquences négatives perçues. L’individu pourra en venir à penser que le sinistre envisagé ne se concrétisera pas, pourra effectuer une ‘comparaison positive’ (avec d’autres individus dans une pire situation), entrer dans le déni et l’évitement (Chen et Zahedi, 2016), et enfin adopter une posture de distanciation (en ne se sentant pas concerné) (Lazarus et Folkman, 1984).

Le tableau 5 ci-dessous montre les catégories d’efforts centrés-émotion associées aux stratégies de ‘gestion de la perturbation’ et de préservation de soi.

<table>
<tr><th colspan="2">Disturbance Handling</th><th>Self-Preservation</th></tr>
<tr><td>Positive reappraisal</td><td rowspan="2">Positive comparison</td><td>Consequences minimization</td></tr>
<tr><td>Threat minimization</td><td>Avoidance</td></tr>
<tr><td></td><td></td><td>Selective attention</td></tr>
<tr><td></td><td></td><td>Distancing</td></tr>
<tr><td></td><td></td><td>Passive acceptance</td></tr>
</table>

**Tableau 5. Les catégories d’efforts centrés-émotion**
(adapté de la ‘Ways of Coping Checklist’ de Lazarus et Folkman (1984),
d’après Beaudry et Pinsonneault, 2005)

Le CMUA prévoit enfin une récursivité qui va matérialiser des spirales positives et négatives de cycles d'appréciation - d'adaptation - de résultats. Ces spirales pourront entrainer soit un renforcement des appréciations (qui seront de plus en plus positives ou négatives) soit une inversion des appréciations (qui passeront de négatives à positives ou vice-versa).

### *1.3.4. Publications et travaux basés sur le CMUA*

Parallèlement à nos articles conceptuels sur le BYOD en tant qu'adoption inversée, présentant des avantages et des risques et pouvant générer des paradoxes de sécurité, nous avons lancé plusieurs études quantitatives sur le terrain. La première concernait des salariés d'entreprises et a été lancée en juin 2017, la seconde portait sur des dirigeants et cadres en entreprise, et s'est déroulée durant le mois de mai 2018.

Nos objectifs étaient (1) de vérifier si le CMUA pouvait entièrement être opérationnalisé de manière quantitative, sans passer par l'entremise de scénarios comme dans les travaux de Elie-dit-Cosaque et Straub (2011), (2) d'identifier les facteurs conditionnant les stratégies de coping des deux types d'acteurs impliqués dans l'adoption inversée (dirigeants et cadres d'un côté et salariés de l'autre), (3) de pouvoir éventuellement comparer les deux types d'acteurs, (4) d'identifier d'éventuels paradoxes de sécurité, et (5) de pouvoir si possible comparer le CMUA avec la PMT sur leur élément commun, c'est-à-dire la stratégie centrée-problème découlant d'une appréciation des menaces.

A ce jour, le point 1 (*opérationnalisation*) est réalisé, et même si d'autres articles pourraient en résulter, le point 2 (*facteurs*) a donné lieu à une publication sur les salariés (JGIM, 2020) et à une conférence (AIM, 2018) sur les premiers résultats concernant les dirigeants de PME. Un article issu de la conférence est aussi en cours d'évaluation. Le point 4 (*paradoxes*) a été partiellement traité dans JGIM, 2020 (voir ci-après) tandis que les points 3 (*comparaison salariés/dirigeants*) et 5 (*comparaison CMUA/PMT*) sont encore à l'état de projets de publications à venir.

#### *1.3.4.1. L'article JGIM, 2020*

Cet article a pour titre « *Coping Strategies and Paradoxes Related to BYOD Information Security Threats in France* ». Il a été publié dans le Journal of Global Information Management.

L'article vise à contribuer à la recherche académique selon trois aspects ('gaps' dans notre papier). Le premier correspond au fait qu'aucune étude n'a abordé les comportements de protection des employés relatifs à leurs propres informations et outils dans le contexte professionnel du BYOD. Le second correspond au fait qu'en SSI, de nombreuses études ont examiné le comportement de protection des employés (stratégies d'adaptation actives et centrées-problème), qui est divisé en deux volets : le respect des politiques de SSI (Moody *et al.*, 2018) et la mise en œuvre de mesures de protection SSI (SIM, 2017). Les études précédentes portaient sur les déterminants de ces stratégies centrées-problème. Cependant, personne n'a expliqué ce qui se passait quand un individu n'agissait pas ou adoptait une stratégie centrée-émotion (plus passive), de la même manière, personne ne s'est intéressé à la mise en regard des déterminants des stratégies centrées-problème face à ceux des stratégies centrées-émotion.

Comme la taille de l'article excédait déjà le nombre de mots maximal autorisé pour un papier dans la revue, répondre aux objections des réviseurs, sur la partie opportunités notamment, aurait développé de manière déraisonnable le nombre de mots. Nous avons donc recentré notre travail sur la partie menaces uniquement et modifié ainsi notre objectif : « *Ce document vise à mieux comprendre les stratégies d'adaptation centrées-problème et centrées-émotion qui découlent des* ***menaces*** *perçues par les employés concernant la sécurité de leurs données personnelles et de leurs outils mobiles* ».

Le troisième élément correspondait à l'identification de paradoxes de sécurité potentiels lors de l'adoption de stratégies de coping découlant de l'appréciation des menaces.

Enfin, nous annoncions l'adoption du CMUA comme modèle de référence pour analyser les stratégies centrées-problème et les stratégies centrées-émotion et leurs antécédents[11]. Cette recherche réalise une opérationnalisation du CMUA à deux niveaux : dans un premier temps, comme la théorie du coping est 'muette' en ce qui concerne l'appréciation primaire, nous avons complété le CMUA, pour sa partie menaces, avec l'appréciation primaire équivalente utilisée dans la PMT.

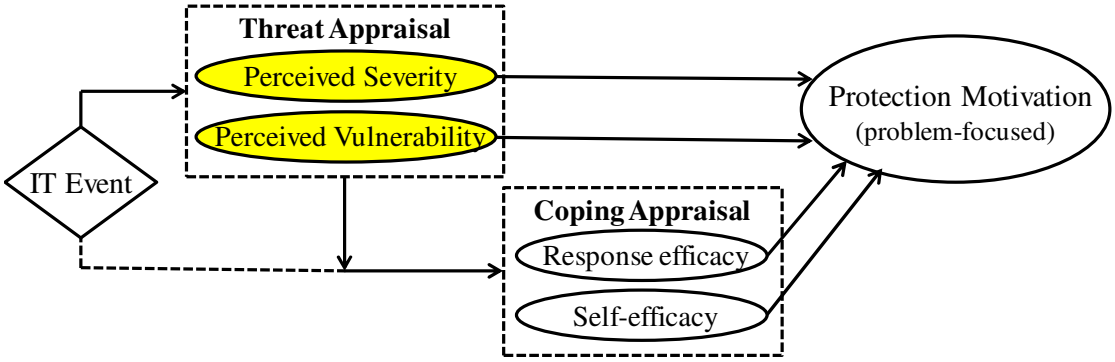


**Figure 13. Les construits permettant l'appréciation des menaces dans la PMT (en jaune)**

Afin de limiter la complexité du modèle, nous avons modélisé l'appréciation de la menace comme un construit de second ordre, constitué par deux construits formatifs de premier ordre empruntés à la PMT, soit respectivement la vulnérabilité perçue et la sévérité perçue (voir figure 13). Pour la prise en compte de la maîtrise perçue des comportements de protection, nous avons pris en compte l'efficacité personnelle (self-efficacy), qui est aussi utilisée dans la PMT. Toujours dans un but de simplification, nous n'avons pas mesuré les comportements centrés-émotion prévus dans le CMUA pour les stratégies de 'disturbance handling'.

Enfin, dans nos définitions des paradoxes de sécurité (security paradoxes), nous évoquions, plus haut, la préoccupation au sujet de la sécurité des informations personnelles (information security concern). Nous avons dérivé ce construit à partir du 'privacy concern', défini comme « *la tendance générale d'un individu à être préoccupé par la confidentialité de ses informations personnelles* » (Li *et al.*, 2011, p.5). Nous avons émis l'hypothèse que l'on pouvait identifier les paradoxes de sécurité en comparant la préoccupation exprimée par un individu avec son appréciation primaire (de la menace) et la pertinence de la stratégie d'adaptation qu'il aura adoptée. Des paradoxes de sécurité pourront donc se produire si des facteurs spécifiques prennent le pas sur d'autres facteurs et amènent les individus à mettre leurs données en péril même après avoir exprimé un niveau de préoccupation élevé (IJIM, 2018 ; Keith *et al.*, 2013 ; Li *et al.*, 2011).

Dans un second temps, comme le CMUA ne donnait pas d'indication précise sur l'opérationnalisation de la maîtrise perçue du comportement, nous avons fait l'hypothèse d'un effet direct sur le choix d'une stratégie de coping, ainsi que l'hypothèse d'un effet modérateur de la maîtrise du comportement sur la relation entre l'appréciation des menaces et le choix de la stratégie de coping.

[11] Nous anticipons de réintroduire l'appréciation des opportunités, qui est l'un des deux gros atouts du CMUA, dans un papier ultérieur.

Ces éléments nous amènent à l'opérationnalisation du modèle du CMUA, pour sa partie menaces, visible en figure 14. On retrouve les trois construits qui complètent le CMUA ; les deux flèches en pointillés matérialisent les effets modérateurs.

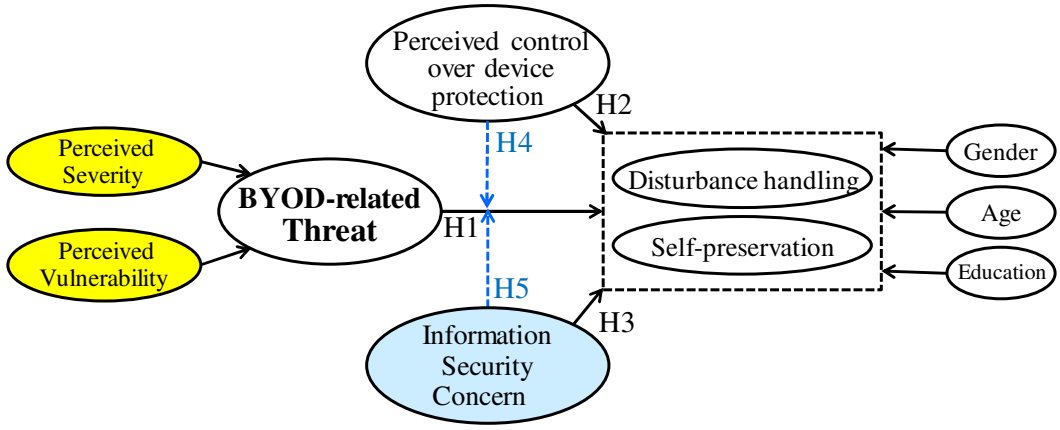


**Figure 14. Le modèle de recherche testé (JGIM, 2020)**

Les questions (items) ont d'abord été discutées lors de trois présentations professionnelles sur le BYOD organisées par les auteurs, puis prétestés au moyen d'entretiens en face à face avec les employés (N = 14). Sur la base des commentaires des personnes interrogées, la lisibilité et la clarté des questions ont été améliorées. Le questionnaire Web a été créé à l'aide de l'outil Qualtrics. Au début du questionnaire, une partie introductive présentait l'objet de l'étude et définissait les principaux termes (BYOD, dispositif personnel, sécurité de l'information, etc.). La participation à l'étude était volontaire et les répondants étaient assurés que les réponses individuelles seraient traitées avec anonymat et confidentialité. L'administration du questionnaire a été sous-traitée à une entreprise en juillet 2017. Deux cent vingt-trois réponses utilisables ont été obtenues. Les données collectées ont été analysées à l'aide de SmartPLS 3.2.7. Après une évaluation positive du modèle de mesure, des construits de second ordre et du modèle structurel, nous avons obtenu les résultats représentés en figure 15.

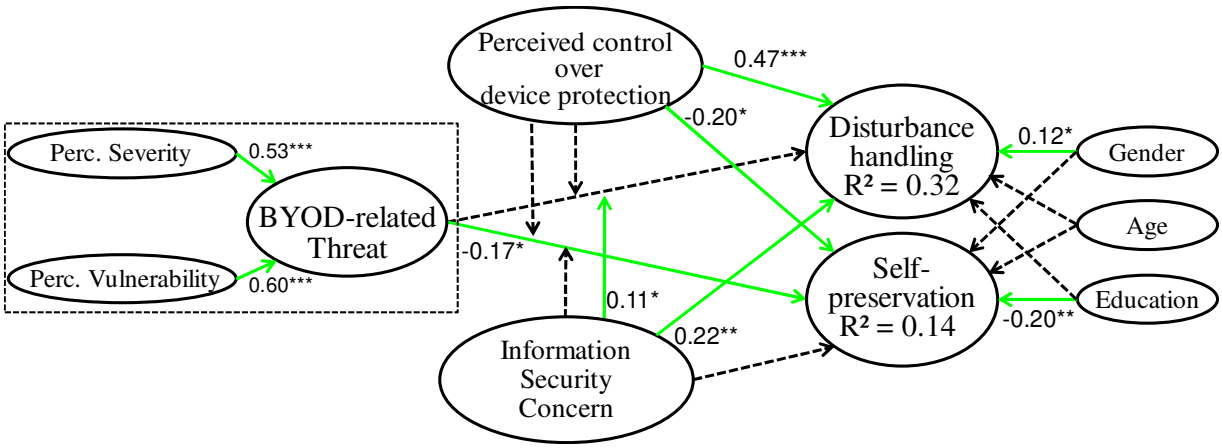


**Figure 15. Résultats et significativité des chemins structurels[12]**

**** p<0.001, ** p<0.01, * p<0.05*

Dans le cas des salariés, on remarque que la maîtrise perçue a des effets uniquement directs, et conformément à nos hypothèses, la maîtrise perçue à une forte influence positive sur l'adoption de stratégies de coping actives et centrées-problème (disturbance handling) et un effet négatif sur l'adoption de comportements passifs (self-preservation). Si la menace perçue décourage les

[12] Les chemins non-significatifs sont en pointillés.

comportements passifs, elle n'encourage pas les comportements actifs. En revanche, une forte préoccupation au sujet de la sécurité des informations personnelles aura un effet modérateur significatif encourageant les comportements actifs, malgré l'effet non-significatif de la menace. La préoccupation aura aussi un effet direct sur l'adoption de comportements actifs.

Nous avons aussi pris en compte la génération des répondants en réalisant des analyses par sous-groupe sur les tranches d'âge correspondant aux générations X (personnes nées avant 1980, N=84) ou Y (les 'digital' natives, N=138). Pour la génération X, la préoccupation pour la sécurité des informations personnelles a un impact négatif plus important sur les comportements passifs ($\beta$= -0,30$^{**}$) que pour la génération Y ($\beta$ = 0,07$^{NS}$). La génération X est plus susceptible de se protéger, car l'évaluation de la menace exerce un impact positif plus fort sur leurs comportements actifs ($\beta$ = 0,36$^{***}$) que sur ceux de la génération Y ($\beta$ = -0,07$^{NS}$). Pour la génération Y, la préoccupation relative à la SSI n'est jamais significative, qu'elle ait un effet direct ou modérateur. La perception d'un événement menaçant n'a aucune influence sur le choix d'une stratégie passive ou active (Palfrey et Gasser, 2013 ; Wang *et al.*, 2015). L'adoption d'une stratégie active est uniquement influencée par la maîtrise perçue de la génération Y. Ces résultats suggèrent un paradoxe de sécurité, dans la mesure où les menaces relatives aux informations personnelles et aux préoccupations de sécurité ne semblent pas avoir d'impact sur cette population.

Les principales contributions théoriques de ce travail sont que cette recherche est la première à aborder les comportements de protection des employés relatifs à leurs informations et outils personnels dans le contexte professionnel du BYOD. À cette fin, le CMUA a été adapté au contexte de la SSI, ce qui a permis de mieux comprendre les stratégies d'adaptation centrées-problème et centrées-émotion. Cette recherche est également la première à la fois à modéliser et à opérationnaliser le CMUA au travers d'équations structurelles et à l'étendre au moyen de variables latentes exogènes pour mesurer l'évaluation de la menace par les individus. Le CMUA a été enrichi par des construits empruntés à la PMT (Rogers, 1983). La maîtrise perçue de la protection a été opérationnalisée avec des effets modérateurs et des effets directs. Les résultats montrent que ses effets sont principalement directs. La préoccupation au sujet de la SSI a été aussi ajoutée au modèle, dans le but de révéler des paradoxes de sécurité, ces phénomènes n'ayant pas encore été étudiés dans le contexte du BYOD. Les résultats montrent que la préoccupation au sujet de la SSI a des effets directs et modérateurs sur les stratégies de coping adoptées.

Sur le plan managérial, une charte pourrait sensibiliser les employés à la nécessité de l'autoformation sur la protection des outils mobiles, ce qui maximiserait l'influence de la maîtrise perçue de la protection. Les entreprises peuvent aussi fournir aux employés des astuces et des pratiques recommandées pour protéger leurs outils mobiles, ce qui peut en conséquence renforcer la sécurité de l'entreprise. Dans le même esprit, développer la perception des menaces potentielles en montrant les problèmes de sécurité les plus courants et leurs impacts potentiels à l'aide d'exemples concrets pourrait réduire les comportements de préservation de soi (centrés-émotion) correspondant au déni ('les risques ne m'affecteront pas') et à la distanciation ('je ne peux rien faire'). Cette étude a montré que lorsque le niveau de préoccupation des employés concernant la SSI est élevé, des paradoxes de sécurité peuvent se produire. Ces paradoxes de sécurité pourraient être réduits par la mise en œuvre de mesures plus contraignantes, telles que des chartes, des politiques BYOD ou des exigences contractuelles spécifiques liées au BYOD.

#### *1.3.4.2. La communication AIM 2018 et l'article en cours d'évaluation par IJIM*

La contribution AIM 2018 reprenait la même étude que le papier précédent, mais portant cette fois sur les dirigeants. Le questionnaire ayant été amélioré, nous avons pu conserver le CMUA complet, c'est-à-dire les parties menaces et opportunités. Toutefois, nous avons éliminé le

construit ‘préoccupation au sujet de la SSI’ (information security concern) car à la suite d’une formation approfondie reçue sur les analyses utilisant les équations structurelles, il s’avère problématique d’utiliser en simultané deux variables modératrices dans un même modèle, du fait d’interactions possibles entre ces deux variables, rendant plus difficile une interprétation. Même s’il est dommage de limiter la compréhension du phénomène étudié du fait de contraintes méthodologiques et techniques, nous avons préféré abandonner notre recherche de paradoxes de sécurité dans l’article qui suit.

Cet article, intitulé « *Bring Your Own Device (BYOD) as a reversed IT adoption: Insights into managers’ Coping Strategies* » est en cours d’évaluation dans la revue ‘International journal of Information Management’ (après rejet d’une soumission initiale à EJIS en février 2019[13]). Il a été écrit en collaboration avec Annabelle Jaouen[14] et Paméla Baillette.

Dans la figure 16 ci-dessous, on retrouve des éléments très similaires à ce qui a été dit précédemment, les nouveautés sont premièrement, l’opérationnalisation de la perception des opportunités en tant que construit de second ordre, formé[15] à partir des construits suivants : l’amélioration des processus métiers ou *business process improvement* (Law et Ngai, 2007), les avantages en termes de coûts ou *cost advantages* (Benlian et Hess, 2011) et l’espoir d’une amélioration de la performance ou *performance expectancy* (Moore et Benbasat, 1991 ; Venkatesh *et al.*, 2003, p. 449). Deuxièmement, l’opérationnalisation du contrôle perçu, ici aussi en tant que construit de second ordre.

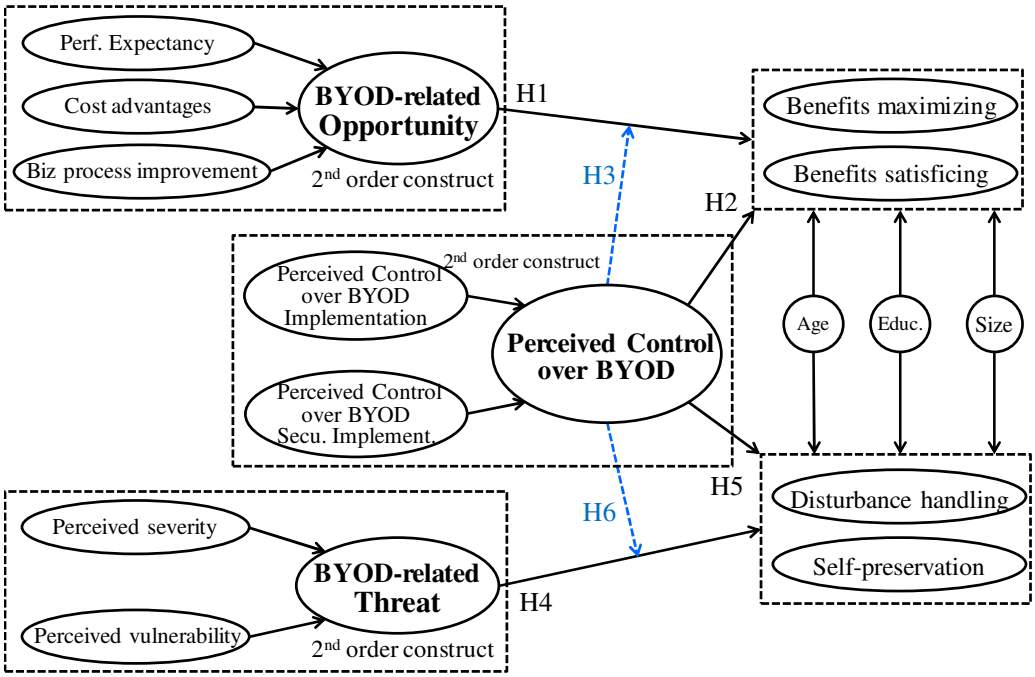


**Figure 16. Le modèle CMUA opérationnalisé pour les dirigeants d’entreprise**

Nous avons utilisé un processus d’enquête très proche du précédent (questionnaire sous Qualtrics administré par une société extérieure). Notre cible était toute personne susceptible de permettre aux salariés d’utiliser leur outil personnel et pouvant décider ou mettre en place des mesures de sécurité pour encadrer cette implémentation d’usages relatifs au BYOD. Trois grandes familles d’acteurs étaient visées : les chefs d’entreprises, les responsables de services

[13] Ce papier a ensuite été soumis à Information & Management puis Decision Support Systems (Rang 1 FNEGE).

[14] Après nos collaborations fructueuses dans le cadre de nos papiers SIM (2017 et 2020) sur la PMT.

[15] De manière formative, sous forme composite (van Riel *et al.*, 2017).

non-informatiques et les responsables de services informatiques (DSI). Cette phase s'est déroulée en mai 2018. Trois cent trente-sept réponses utilisables ont été obtenues. Les données collectées ont été analysées à l'aide de SmartPLS 3.2.8.

Il est à noter que le questionnaire utilisé prévoyait des extensions du CMUA et de la PMT qui seront discutées dans le chapitre suivant. Nous avons aussi décidé d'inclure une question portant sur le fait que l'introduction du BYOD était prévue ou déjà effective dans l'entreprise.

Les résultats les plus saillants proviennent des différences entre ces deux sous-groupes (159 'avant' implémentation, 178 'après' implémentation. Avant la mise en œuvre, les dirigeants peuvent avoir surestimé leurs attentes relatives aux avantages du BYOD et, après la mise en œuvre, ces attentes diminuent, laissant la place à une maîtrise accrue de la mise en œuvre du BYOD, avec un effet positif sur les stratégies maximisant les avantages et des effets négatifs sur les stratégies pour profiter passivement des avantages. Par conséquent, après la mise en œuvre, l'opportunité perçue liée à l'implémentation du BYOD ne fait que favoriser la maximisation des avantages, et les stratégies de satisfaction passives sont abandonnées. Après la mise en œuvre, les menaces perçues favorisent les stratégies de protection centrées-problème et découragent les stratégies de préservation de soi. Un processus d'arrêt-démarrage a lieu, au cours duquel les responsables mettent en œuvre des mesures de sécurité, pensent maîtriser la situation et tendent à cesser de mettre en œuvre d'autres mesures de sécurité jusqu'à ce que de nouvelles menaces soient perçues. De plus, le pouvoir explicatif de nos modèles est accru après mise en œuvre du BYOD pour les stratégies de coping découlant des menaces perçues, tandis qu'il diminue pour les stratégies de coping découlant des opportunités. Ces résultats soulignent l'importance de prendre en compte le moment où l'on se situe dans le processus d'implémentation (avant ou après) dans de telles études.

Cet article en cours d'évaluation pose aussi le problème d'opérationnalisation totale du CMUA, prévu à l'origine pour intégrer un processus itératif, et mis en œuvre dans le cadre d'études qualitatives (Beaudry et Pinsonneault, 2005). Il semble difficile d'intégrer ceci dans un modèle quantitatif dont les données proviennent de questionnaires. En effet, les méthodologies quantitatives correspondent majoritairement à des recherches latitudinales. Or, seule une étude longitudinale portant sur les mêmes acteurs permettrait d'étudier l'évolution de leurs appréciations et réappréciations successives de la situation selon les (et à partir des) stratégies adoptées. Cette problématique apparaît donc comme complexe à intégrer dans le cadre d'une étude quantitative et mérite une réflexion approfondie.

Tout comme dans ce mémoire de HDR, j'envisage de mieux prendre en compte cet aspect dans mes prochains travaux sur le CMUA (1) dans la partie théorique en disant que le CMUA est itératif (2) dans la méthodologie en expliquant la complexité d'une prise en compte de cet aspect et (3) dans les limitations et pistes de recherche, en insistant sur le fait qu'une photographie à un instant 'T' ne reflète pas toute la richesse du CMUA dans l'étude des processus d'appréciation-réappréciation et des stratégies de coping adoptées. Toutefois, le processus d'arrêt-démarrage identifié dans l'article IJIM (R3) illustre dans une certaine mesure l'importance de cet aspect temporel.

### *1.3.5. Conclusion : vers des enrichissements du CMUA*

Nous avons vu que, pour être opérationnalisé dans le cadre d'analyses par les moindres carrés partiels et de la modélisation en utilisant des équations structurelles, le CMUA nécessitait d'être enrichi à plusieurs niveaux.

Premièrement, l'appréciation primaire n'étant pas précisée dans les théories du coping, l'appréciation des opportunités nécessite d'être enrichie selon le contexte, qui peut avoir trait à la technologie mise en place (BYOD ou logiciel par exemple) ou aux personnes interviewées

(salariés ou décideurs par exemple). Pour l'appréciation des menaces, dans le domaine de la sécurité, les deux construits de la PMT (impact potentiel et probabilité) nous paraissent tout à fait adaptés. Le fait de créer des construits de second ordre permet de rester conforme à la théorie et d'éviter d'alourdir les modèles.

Pour la maîtrise du comportement, nous avons utilisé l'efficacité personnelle (self-efficacy) en tant que variable modératrice, mais la PMT prévoit aussi l'efficacité perçue du comportement (response efficacy) qui mériterait d'être incluse dans le CMUA.

Nous avons été obligés d'écarter de nos analyses certains items permettant de mesurer la stratégie de coping adoptée, surtout pour les comportements centrés-émotion. En effet, nous nous sommes trouvés confrontés à des problèmes de validation de notre instrument de mesure soit au niveau de la pondération des items, soit au niveau de la cohérence interne (fiabilité composite) des construits. Les remèdes à ces problèmes sont (1) l'amélioration de la cohérence des comportements unitaires pris en compte (déni, distanciation, etc.) et (2) une augmentation du nombre d'items, pour s'assurer d'avoir au moins deux items valides, malgré des rejets éventuels.

Enfin, un réviseur a émis en remarque que le CMUA était un modèle itératif (Beaudry et Pinsonneault, 2005). Cette récursivité nous semble difficile à mettre en place dans une enquête par questionnaire, d'ailleurs Elie-Dit-cosaque et Straub (2011) n'ont pas non plus intégré cette réappréciation de la situation après chaque phase d'adaptation. Toutefois, l'adoption d'une « mixed-method » (Annansingh et Howell, 2016 ; Venkatesh *et al.*, 2013) permettrait de prendre en compte l'aspect itératif du CMUA, en tablant sur les avantages combinés des méthodes quantitatives ET qualitatives. Par contre, il deviendrait néanmoins plus difficile de valider le modèle théorique du CMUA d'un point de vue statistique.

Que ce soit pour le CMUA ou la PMT, nous allons envisager d'autres améliorations possibles, c'est-à-dire discuter de l'enrichissement de ces modèles basés sur le coping, non seulement en ayant recours à d'autres variables indépendantes (en amont), mais aussi à d'autres variables dépendantes (en aval), c'est-à-dire à d'autres familles de comportements.

# 2. Enrichissement des modèles, ouvertures et projets

Dans une première partie, nous verrons les pistes qui peuvent être explorées pour enrichir les deux modèles étudiés basés sur le coping, respectivement la PMT et le CMUA. Dans une seconde partie, nous verrons les autres thèmes sur lesquels j'ai travaillé, les thèses déjà co-encadrées ainsi que des ouvertures vers d'autres pistes de recherche et d'encadrement.

## 2.1. Enrichissements des modèles basés sur le coping

Ces enrichissements peuvent se faire en amont, par des ajouts de variables indépendantes, et en aval, en s'intéressant à d'autres types de comportements et stratégies de coping.

### *2.1.1. En amont du coping (variables indépendantes)*

#### *2.1.1.1. Pistes d'enrichissements de la PMT*

Dans un premier temps, certains construits tirés des théories de l'acceptation et de l'utilisation des technologies de l'information déjà envisagées dans ma thèse et les travaux qui en ont découlé, paraissent tout à fait pertinents (voir aussi le tableau 3).

J'ai déjà intégré avec succès *l'influence sociale* (normes subjectives) tirée de la TPB et de l'UTAUT notamment dans l'article SIM de 2017. J'ai aussi tenté d'intégrer, sans succès à ce jour *l'habitude*. Pourtant, Limayem et Hirt (2003, 2007) ont montré l'influence de *l'habitude* sur les comportements d'adoption. Prendre en compte *l'habitude* reste d'actualité et j'envisage de la réintroduire ultérieurement dans mes travaux car j'ai constaté (SIM, 2008) que la routinisation des comportements était très importante dans l'adoption durable de comportements relatifs à la SSI. De nombreux spécialistes vont aussi dans ce sens, en considérant l'habitude comme le 'graal' des comportements relatifs à la SSI. Dans nos études avec P. Baillette sur le CMUA, nous avons aussi intégré la *préoccupation au sujet de la sécurité de l'information* (information security concern), qui pourrait compléter l'appréciation des menaces.

En plus de ces construits, deux théories me paraissent pertinentes pour enrichir les modèles basés sur le coping : la théorie des liens sociaux et, principalement pour les dirigeants d'entreprise, la théorie néo-institutionnelle.

*La théorie des liens sociaux* (SBT) ou 'social bond theory' (Gottfredson et Hirschi, 1990 ; Jenkins, 1997) postule qu'une personne adopte un comportement délinquant quand l'insuffisance de liens sociaux lui en laisse la liberté. La théorie est basée sur quatre construits qui sont réutilisables dans le contexte de la SSI : *l'attachement* à l'entreprise (qui pourrait expliquer des comportements pour préserver son entreprise), le sens du *devoir* (une responsabilité en SSI plus grande), *l'implication* dans le travail (qui évite de 'mauvaises actions'[16], comme prendre des risques en surfant sur des sites sensibles), les *croyances* dans les normes et l'autorité (pour respecter une charte de SSI par exemple). À notre connaissance, mis à part notre travail dans SIM (2008), la SBT n'a été utilisée que quatre fois pour l'analyse du comportement des salariés en SSI (Cheng *et al.*, 2013 ; Feng et al., 2019 ; Ifinedo, 2014 ; Safa *et al.*, 2016).

La figure 17 ci-dessous donne un aperçu du modèle qui pourrait être étudié. On note que des construits de second ordre pourraient simplifier ce modèle.

[16] Au sens d'Agnew (1995).

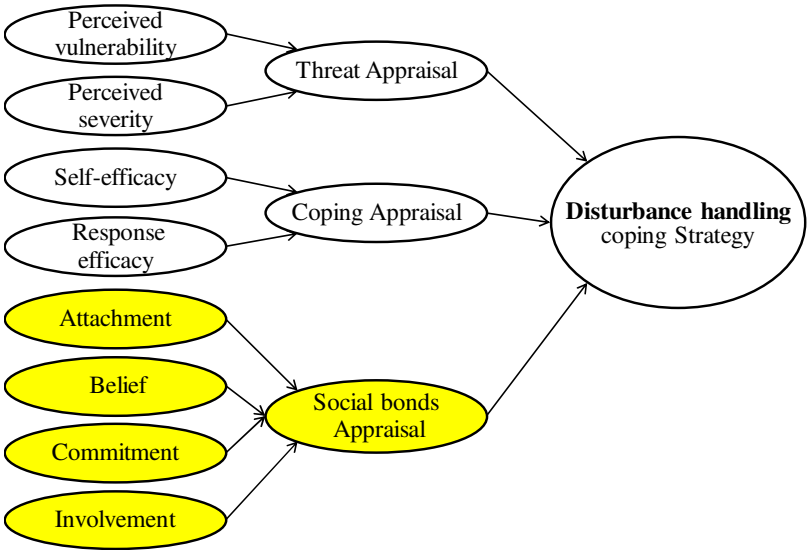


**Figure 17. La PMT enrichie par la SBT (en jaune)**

*La théorie néo-institutionnelle* (DiMaggio et Powell, 1983 ; Meyer et Rowan, 1977). Ces auteurs identifient trois types d'isomorphisme institutionnel : coercitif (*coercive*), mimétique (*mimetic*) et normatif (*normative*). Hu *et al.* (2007) ont montré que la théorie néo-institutionnelle est particulièrement pertinente pour expliquer le changement de comportement au niveau organisationnel.

L'isomorphisme *coercitif* se produit lorsque les organisations subissent « *les pressions formelles et externes exercées sur elles par d'autres organisations dont elles sont dépendantes, ainsi que les attentes culturelles de la société dans laquelle elles évoluent* » (DiMaggio et Powell, 1983, p.150). Cavusoglu *et al.* (2015) ont postulé qu'en sécurité de l'information les pressions coercitives sont exercées principalement via deux sources : les partenaires commerciaux et les normes de sécurité. Elles peuvent également découler de politiques gouvernementales ou provenir d'associations ou de réseaux professionnels (Liang *et al.*, 2007)

L'isomorphisme *mimétique* se produit quand des organisations imitent d'autres organisations. Ceci est particulièrement évident dans les environnements incertains, car cela minimise les risques (Hu *et al.*, 2007). De même, on peut s'attendre à ce que les organisations soient préoccupées par le fait que leurs dépenses en matière de sécurité de l'information soient en phase avec celles de leurs concurrents (Cavusoglu *et al.*, 2015).

L'isomorphisme *normatif* résulte de la professionnalisation des acteurs organisationnels, tels que les dirigeants d'organisations et de services (Hu *et al.*, 2007). Les organisations sont susceptibles d'ajuster leur comportement sur ce qui est considéré comme approprié par les membres de leurs réseaux sociaux, notamment leurs partenaires commerciaux et les associations professionnelles, et donc d'adopter des techniques et méthodes qui reflètent les normes actuelles de ces réseaux (Cavusoglu *et al.*, 2015). Les pressions normatives peuvent être transmises lors de la participation à des événements, tels que des conférences ou des ateliers organisés par des associations professionnelles. Les normes de sécurité de l'information sont perçues comme utiles, car elles permettent de démontrer l'engagement de l'institution dans l'amélioration de ses pratiques de sécurité (Cavusoglu *et al.*, 2015).

La théorie néo-institutionnelle a été utilisée avec succès non seulement en SI, mais aussi pour expliquer certains comportements relatifs à la sécurité de l'information (Angst *et al.*, 2017 ; Cavusoglu *et al.*, 2015 ; Daud *et al.*, 2018 ; Hu *et al.*, 2007 ; Spears *et al.*, 2013).

En 2016, nous avions démarré un projet qui est resté en stand-by depuis, intégrant les trois forces mimétique, normative, et coercitive de la théorie néo-institutionnelle. Nous maintenons

néanmoins que pour les dirigeants d'entreprise notamment, les forces de pression institutionnelles pourraient jouer un rôle important dans la mise en place de mesures de sécurité. En conséquence, les éléments en figure 18 ci-dessous peuvent enrichir la PMT en remplaçant les construits de la SBT en figure 17.

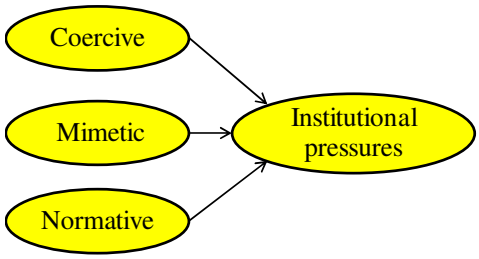


**Figure 18. La théorie néo-institutionnelle (adapté de DiMaggio et Powell, 1983)**

*2.1.1.2. Pistes d'enrichissements du CMUA*

Le CMUA pourrait aussi inclure certains des éléments examinés ci-dessus, en modélisant soit un effet direct, soit un effet modérateur. Du fait des contraintes techniques imposées par l'existence de plus d'une variable modératrice, il faudrait passer par des variables de second ordre comme représenté dans l'exemple ci-dessous, en figure 19.

Dans nos précédents travaux sur le CMUA, nous avions utilisé l'efficacité personnelle (*self-efficacy*). Mais en toute logique, il est possible d'inclure aussi l'efficacité de la réponse (*response efficacy*) tirée aussi de la PMT, qui resterait compatible théoriquement avec le CMUA, puisqu'elle matérialiserait la maîtrise perçue des conséquences du comportement (*perceived control over behavioral outcomes*). Pour éviter d'avoir deux variables modératrices, dont les interactions pourraient biaiser les résultats, ces construits représenteront les composantes formatives d'un construit de second ordre 'maîtrise perçue du comportement' (*perceived behavioral control)*, en figure 19.

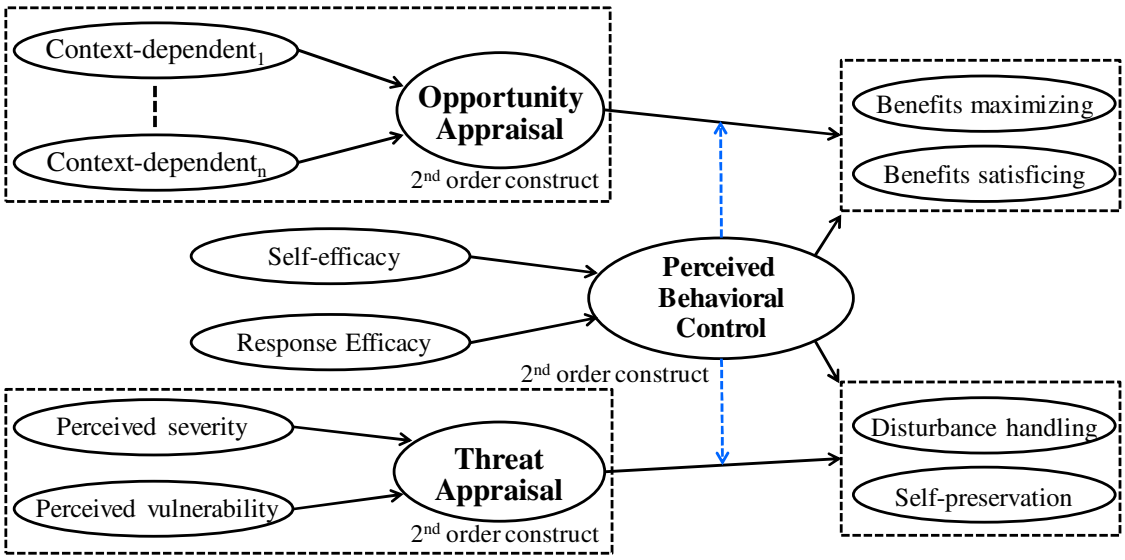


**Figure 19. Opérationnalisation[17] du CMUA avec plusieurs construits ayant un effet modérateur**

[17] Nous avons laissé 'vides' les construits relatifs à l'appréciation des opportunités, pour matérialiser le fait qu'ils seront adaptés au contexte et aux acteurs étudiés.

### *2.1.2. En aval du coping (variables dépendantes)*

Les théories du coping peuvent aussi être adaptées pour intégrer de nouveaux comportements résultants. Concernant la PMT, on peut s'intéresser à d'autres comportements centrés-problème, comme le déclenchement du 'soutien de la direction' ou encore des comportements 'directs ou indirects'. On peut aussi étendre la PMT à l'étude de comportements centrés-émotion.

Le CMUA, intégrant des opportunités confrontées à des menaces, pourrait être utilisé pour la détection de paradoxes, comme nous avons déjà tenté de le faire dans nos travaux précédents sur la sécurité de l'information (JGIM, 2020). Le technostress pourrait représenter l'une des conséquences des comportements centrés-émotion résultant de l'appréciation d'un évènement en tant que menace, dans le cas où la maîtrise perçue du comportement nécessaire est faible.

#### *2.1.2.1. Pistes d'enrichissements de la PMT*

Je vois trois principales pistes : (1) l'explication d'autres familles de comportements centrés-problème, (2) l'ajout de comportements centrés-émotion et enfin (3) le choix d'expliquer l'intention comportementale ou bien le comportement lui-même, selon le type de comportement à expliquer (par exemple dans le cas de comportements récurrents).

Premièrement, si le but premier de la PMT est d'expliquer la motivation à la mise en place de mesures de sécurité, certains auteurs ont travaillé, toujours sur les comportements centrés-problème, dans le cadre des aspects 'non-action', c'est-à-dire les 'omissive behaviors' (Moser *et al.*, 2011 ; Workman *et al.*, 2008).

La PMT pourrait être utilisée pour expliquer d'autres comportements centrés-problème, comme le soutien du dirigeant (TMS) ou 'top management support'. Le soutien du dirigeant inclut plusieurs notions, telles que l'implication et la participation (Kulkarni *et al.*, 2017). Les actions de soutien peuvent être classées en trois types principaux, à savoir la *participation*, *l'implication* et *l'allocation de ressources* (Liu *et al.*, 2015). La participation des dirigeants peut permettre de résoudre des problèmes de gestion et d'adapter des structures ou des processus organisationnels inadéquats. L'implication correspond à l'état psychologique du dirigeant qui doit participer de manière sincère et volontaire, essentielle au succès d'un projet (Dong *et al.*, 2009). Un dirigeant pourra allouer des fonds, valider des budgets, et affecter des ressources matérielles et humaines à un projet SI et ainsi créer un contexte de soutien. Le TMS peut également se traduire par la promotion du projet (Lin *et al.*, 2014 ; McComb *et al.*, 2008) et un soutien sans équivoque des personnes affectées au projet (Boonstra, 2013, p. 500).

Le soutien du dirigeant peut par exemple être mesuré au travers des items suivants :

- Je *valide* régulièrement les *mesures* de SSI proposées par la personne qui s'en occupe dans mon entreprise ;
- Je *valide* régulièrement les *budgets* de SSI proposés par la personne qui s'en occupe dans mon entreprise ;
- Je *soutiens* régulièrement *la personne* qui s'en occupe dans mon entreprise ;
- Je *sensibilise* régulièrement *mes employés* aux mesures de sécurité des SI.

Le modèle mettant en perspective ces deux types de comportement est représenté en figure 20.

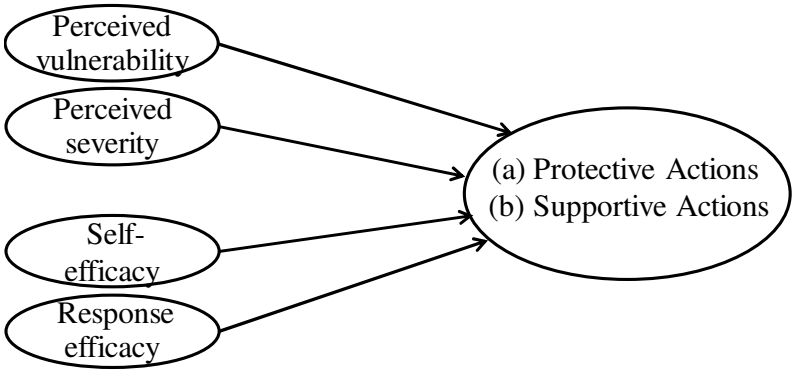


**Figure 20. La PMT intégrant le TMS**

Nous avons co-écrit avec Annabelle Jaouen un article (SIM, 2019) intitulé « *Information Security in SMEs: Determinants of CEOs' Protective and Supportive Behaviors* », qui vient d'être publié. Il a pour but d'examiner dans quelle mesure les déterminants de la PMT vont influencer les comportements de protection (protective actions) et les comportements de soutien (supportive actions) des dirigeants de PME. Au modèle précédent, nous avons ajouté l'influence sociale car des recherches sur la PME ont montré que les dirigeants s'appuient souvent sur leurs réseaux sociaux et professionnels pour prendre des décisions. De telles influences sociales peuvent donc constituer une variable pertinente pour expliquer les comportements des dirigeants (Ozgen et Baron, 2007 ; Schoonjans *et al.*, 2013 ; SIM, 2017).

Nous réalisons une comparaison des influences de ces déterminants sur les comportements de protection et de soutien, et nous discutons des divergences entre leurs effets.

Nos principaux résultats sont tout d'abord que les effets de la vulnérabilité perçue et de l'efficacité perçue de la réponse sont quasi identiques. Les effets des trois autres variables sont bien plus différenciés. On note que l'effet de la gravité perçue (perceived severity) sur les actions de protection est quasi nul et non significatif, alors que son effet sur les actions de soutien est significatif et beaucoup plus fort ($\beta$=0,20$^{**}$). Ceci permet de supposer que la gravité perçue est une source d'implication pour le dirigeant, qui va apporter son soutien, même si cela ne se traduit pas en actions de protections 'directes'. Ensuite, l'efficacité personnelle a un effet bien plus marqué sur les actions protectives que sur les actions de soutien du dirigeant ($\beta$=0,31$^{***}$ contre 0,14$^{*}$). Ce fait peut s'expliquer par la difficulté plus importante des actions de protection comparées au soutien de ces actions. Enfin, l'influence sociale a un effet plus important sur les comportements de soutien que sur les actions protectives. De plus, l'influence sociale est le construit qui a le plus d'effet sur les comportements de soutien. Cela signifie que les relations du dirigeant jouent un rôle crucial dans le renforcement de la SSI d'une entreprise, car même si les dirigeants n'agissent pas directement faute de compétences par exemple, ils vont soutenir les personnes qui se chargent de la SSI, valider les projets et budgets, et sensibiliser les salariés.

Ces résultats présentent des apports managériaux importants, car nous voyons que le niveau de SSI d'une entreprise n'est pas seulement une affaire de mise en place de mesures de sécurité plus ou moins techniques, mais qu'il va aussi dépendre de l'implication et du soutien du dirigeant, sachant que le soutien est lui-même déclenché majoritairement par le réseau professionnel du dirigeant.

Sur le plan théorique, nous montrons que non seulement la PMT peut être utilisée pour expliquer d'autres comportements que des actions directes, mais que le pouvoir explicatif de la PMT reste satisfaisant quand il est appliqué au cadre des comportements de soutien. De plus, les construits de la PMT ont majoritairement révélé une influence différenciée sur les deux

types de comportements. Nous contribuons donc non seulement à la littérature sur la PMT, mais aussi à la littérature sur les comportements de soutien, qui à notre connaissance n'ont jamais été examinés dans le cadre de la SSI, mis à part dans l'étude qualitative menée dans mon article SIM de 2012.

Une deuxième piste d'enrichissement de la PMT vise à pallier une de ses principales faiblesses. En effet, nous avons vu précédemment que la PMT ne permet pas, en l'état, de prendre en charge les comportements centrés-émotion. D'où l'idée de revenir à la base des théories du coping pour enrichir PMT avec ce type de comportements. Par exemple, Moody *et al.* (2018) montrent l'adaptation à la SSI de l'extended parallel processing model (EPPM) de Witte (1992), qui introduit les concepts intéressants d'évitement (avoidance) et de réactance (reactance) correspondant à deux mécanismes fréquemment adoptés dans le cadre de *l'adaptation émotionnelle* à une menace. *L'évitement* est une réponse comportementale qui a pour but de contrôler la peur, il correspond au fait d'ignorer des informations ou des éléments qui susciteraient la peur afin de ne pas ressentir de peur. La *réactance* fait référence à une volonté établie de rejeter les informations et autres éléments susceptibles de susciter la peur, amenant ainsi l'individu à activement ne pas croire et remettre en question la ou les causes de la peur.

On peut aussi se baser sur le CMUA pour enrichir la PMT avec les comportements centrés-émotion (voir tableau 5). Enfin, le très récent article de Liang et al. (2019) examine les comportements centrés-problème et centrés-émotion dans le cas de menaces relatives aux TI. La figure 21 ci-dessous montre comment l'on peut complémenter la PMT, sachant que l'on peut de plus adapter les échelles de mesures utilisées dans les études sur le CMUA, l'article de Liang et al. (2019, p. A7), le WCQ[18] ou encore le COPE inventory[19] pour mesurer l'adoption de ces stratégies de coping.

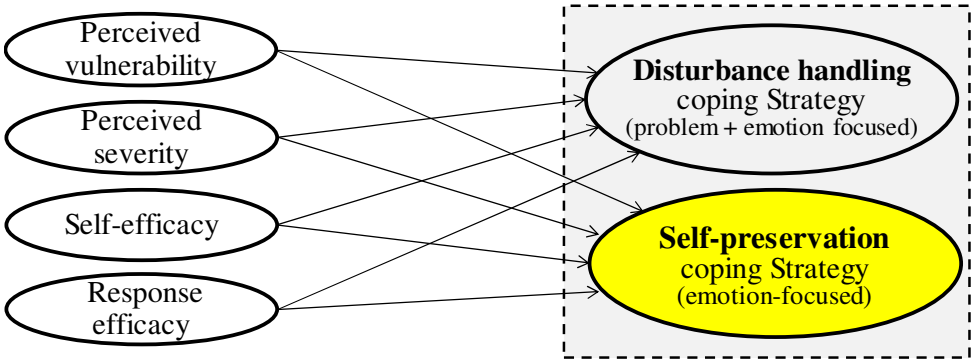


**Figure 21. La PMT complétée pour étudier des comportements centrés-émotion**

Pour terminer sur les enrichissements en aval de la PMT, je tiens à discuter d'une question qui revient souvent lors de son utilisation, car la réponse peut conditionner certains choix de modèles : la PMT explique-t-elle mieux les intentions comportementales ou bien les actions, c'est à dire les comportements eux-mêmes ?

Si l'on en revient aux définitions d'origine, la PMT a pour but d'expliquer « *la décision (ou l'intention) d'initier, de poursuivre ou d'inhiber les réponses adaptatives applicables (ou les comportements d'adaptation)* » (Floyd *et al.*, 2000, p. 411). Même si la PMT suppose « *que la motivation à la protection est mieux mesurée par des intentions comportementales* » (Rogers, 1983, p. 172), cette théorie « *est suffisamment ouverte pour s'appliquer à toute situation*

[18] Ways of coping questionnaire (Lazarus et folkman, 1984, p. 328).
[19] COPE Inventory (Carver et al., 1989, p. 272).

*impliquant une menace* » (Rogers, 1983, p. 172), que ce soient des comportements correspondant à des actes uniques, répétés ou multiples (Prentice-Dunn et Rogers, 1986).

Par conséquent, en fonction du type de comportement étudié, les travaux académiques basés sur la PMT (voir Annexe 2) ont exploré de manière équilibrée : l'intention comportementale pour 14 études (Crossler *et al.*, 2019 ; Jansen et van Schaik, 2018 ; Moody *et al.*, 2018), le comportement réel pour 11 études (Li *et al.*, 2019 ; Torten *et al.*, 2018) ou les deux pour 13 études (Mwagwabi *et al.*, 2018 ; Thompson *et al.*, 2017).

Même si la PMT aboutit à de meilleurs résultats avec l'intention comportementale, certains auteurs préconisent de mesurer le comportement réel, car cela évite que la recherche aboutisse à des conclusions basées seulement sur des possibilités (Limayem *et al.*, 2007), d'autres considèrent qu'un comportement réel est plus objectif qu'une intention comportementale (Ng *et al.*, 2009). Au-delà de ces arguments, c'est plus le contexte de l'étude qui importe selon moi : si l'on étudie des comportements qui peuvent être répétitifs, la prise en compte de l'intention n'est plus pertinente (Crossler et Bélanger, 2014). C'est pourquoi dans certains de nos travaux, nous avons étudié l'intention qui exerce une influence sur l'action (SIM, 2017) et dans d'autres uniquement l'action (SIM, 2019), car les comportements étaient répétitifs. Ceci renvoie aussi au débat sur les liens entre l'attitude comportementale, l'intention comportementale et le comportement lui-même (Anderson & Agarwal, 2010 ; Chandon *et al.*, 2006 ; Crossler *et al.*, 2013 ; Van Gelderen *et al.*, 2015). De plus, selon les théories énactivistes (Mohd Salleh *et al.*, 2017 ; Varella *et al.*, 1992), le comportement peut également renforcer les intentions et les motivations. C'est donc aussi dans le cadre des interrelations et d'un bouclage entre intentions et actions que les comportements relatifs à la SSI pourraient gagner à être étudiés.

#### *2.1.2.2. Pistes d'enrichissements du CMUA*

Si le CMUA intègre déjà les comportements centrés-émotion, la palette des comportements visible dans le tableau 5 n'a pas été entièrement testée dans le cadre de ce modèle (JGIM, 2020 ; IJIM, R3 ; Liang *et al.*, 2019 ; Elie-Dit-Cosaque et Straub, 2011 ; Chen et Zahedi, 2016). Toutefois, une contrainte se pose : comme le CMUA vise à expliquer le comportement de quatre variables dépendantes, même si l'on n'a que 3 items par variable, le chercheur doit gérer douze items, donc 12 questions, sans compter les variables indépendantes. Si l'on détaille les comportements centrés-émotion, on pourra très rapidement passer à une vingtaine, voire une trentaine de questions, toujours uniquement pour les variables dépendantes ! Ce qui ferait qu'un questionnaire pourrait devenir très long et décourager les répondants.

J'envisage donc de tester dans un premier temps un modèle allégé. Dans un souci de simplification, seule la partie correspondant aux menaces est visible en figure 22 ci-dessous. Nous remarquons qu'il faut 11 items (traits en partie droite), soit 17 items en tout si l'on prévoit un minimum de 6 items pour les deux stratégies de coping relatives aux opportunités. On peut noter que la comparaison positive (*positive comparison*) est commune aux deux types de stratégies (Beaudry et Pinsonneault, 2005) et semble difficile à intégrer dans un modèle structurel. Des travaux ultérieurs pourraient tester cette intégration.

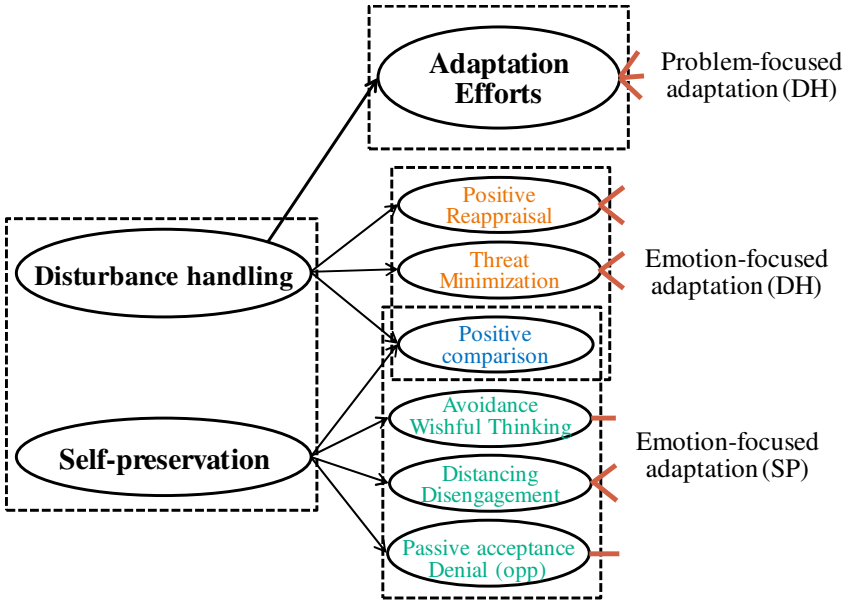


**Figure 22. Exemple de comportements centrés-émotion[20]**

Nous avons aussi utilisé le CMUA pour tenter d'identifier des paradoxes de sécurité, en mettant en regard les appréciations 'menaces' et 'opportunités', et en intégrant la préoccupation vis-à-vis de la SSI. Cela a donné lieu à plusieurs travaux, présentés lors du Pré-ICIS 'WISP' 2016 et de l'AIM 2017, ainsi qu'à une publication dans JGIM (2020).

Une autre piste intéressante est l'étude du *technostress* en matière de sécurité de l'information. Le technostress a déjà été traité en systèmes d'information (Ayyagari *et al.*, 2011 ; Ragu-Nathan *et al.*, 2008 ; Tarafdar *et al.*, 2007 ; Srivastava *et al.*, 2015) et fait l'objet d'une attention croissante en SSI. Si la majorité des études s'est intéressée au technostress provoqué par la nécessité pour les employés de respecter les mesures de sécurité (d'Arcy *et al.*, 2014 ; Lee *et al.*, 2016 ; Park et Cho, 2016), ou encore à l'impact négatif du technostress sur le respect des mesures de sécurité (Hwang et Cha, 2018), il n'en reste pas moins que le technostress en matière de sécurité de l'information, appelé aussi le 'security-related stress' (stress relatif à la sécurité) reste négligé dans la littérature sur le technostress (Ament et Haag, 2016).

Les études sur le technostress sont principalement basées sur les construits suivants :

- La *techno-complexité* : les employés doivent investir du temps et des efforts pour comprendre et apprendre à travailler avec les TI. Ainsi, la confusion résulte du jargon, de la multiplicité des fonctions, etc.
- La *techno-insécurité* : la pression d'une perte d'emploi éventuelle pour une personne devant améliorer sa compréhension des nouvelles fonctionnalités des TI est permanente pour les employés.
- La *techno-invasion* : les employés sont toujours connectés, ils peuvent donc être contactés à n'importe quel moment ou endroit. Leur vie professionnelle tend à se confondre avec leur vie personnelle.
- La *surcharge technologique* : les employés doivent accomplir plus de travail en moins de temps et sont confrontés à plus de nouvelles données qu'ils ne peuvent en gérer ou utiliser. De plus, cela implique des interruptions et du multitâche.
- La *techno-incertitude* : une transition technologique permanente empêche les employés de développer une base expérientielle. Ils doivent régulièrement actualiser leurs savoirs.

[20] Dans le récent article de Liang et al. (2019), les trois derniers comportements centrés-émotion correspondent à des stratégies 'Inward EFC' (p. 382). Les stratégies 'Outward EFC' correspondant à des comportements d'évacuation des émotions (venting) et la recherche de soutien émotionnel.

Encore une fois, nous souhaitons nous recentrer sur les dirigeants d'entreprise, qui constituent pour nous une population spécifique. Si effectivement, certaines pressions (comme celles de la théorie néo-institutionnelle) peuvent créer un technostress ou un stress relatif à la sécurité, nous partons du principe qu'un dirigeant ou un cadre d'entreprise qui sait qu'il doit mettre en place des mesures de sécurité et qui ne les met pas en place, va entrer dans un processus centré-émotion qui va constituer une source de stress. Il s'agit donc pour nous de compléter ou d'affiner certains des comportements de coping étudiés par Lazarus (1966) puis par Beaudry et Pinsonneault (2005 ; 2010) pour matérialiser et mesurer ce stress.

Par exemple, un dirigeant qui perçoit une forte probabilité et un fort impact (*perceived severity* et *vulnerability*) potentiels d'une atteinte à la sécurité des informations de son entreprise et qui, au lieu d'agir, va entrer dans une stratégie de coping centrée-émotion de préservation de soi (self-preservation) correspondant à des émotions d'anxiété, de peur, de détresse ou de préoccupation, va donc ressentir un stress relatif à la sécurité de ses informations. Nous envisageons de bâtir un instrument de mesure de ce stress relatif à la sécurité, adapté aux dirigeants et décideurs. Cet instrument de mesure s'avère très spécifique, et en conséquence devra être bâti à partir de construits différents de ceux mesurant le technostress classique.

### *2.1.3. Conclusion sur les enrichissements et projets relatifs aux théories du coping*

Nous avons vu qu'en amont des théories du coping, des construits tels que l'habitude ou des théories comme la théorie des liens sociaux (SBT) ou la théorie néo-institutionnelle peuvent enrichir la PMT et le CMUA. En aval de ces théories, des comportements de soutien (top management support) peuvent être aussi étudiés.

Nous avons aussi montré que la PMT, théorie de référence en SSI, gagne à être complétée par des stratégies de coping plus centrées-émotion, car s'il est important de savoir si les individus vont agir en termes de sécurité de l'information, il est tout aussi important de savoir quels facteurs caractériseront des comportements plus passifs.

A ce sujet, nous avons proposé un article pour la conférence de l'AIM en 2019 (AIM, 2019) qui a deux objectifs : le premier, que nous ne détaillerons pas ici, correspond à des considérations méthodologiques, c'est-à-dire que nous faisons un point sur les dernières recommandations (1) sur les justifications à donner pour démontrer la qualité des modèles utilisés en équations structurelles, et (2) en matière de comparaison de comportements de modèles structurels. Le deuxième objectif est de mettre en perspective les apports croisés de la PMT et du CMUA, sur leurs points communs, c'est-à-dire l'explication de comportements basés sur une appréciation primaire des menaces.

Nous avons donc comparé le modèle visible en figure 21, c'est-à-dire la PMT enrichie avec des comportements centrés-émotion, avec le modèle en figure 23 ci-dessous, c'est-à-dire le CMUA 'partie menaces' enrichi des construits de la PMT (hors des pointillés qui représentent les construits propres au CMUA).

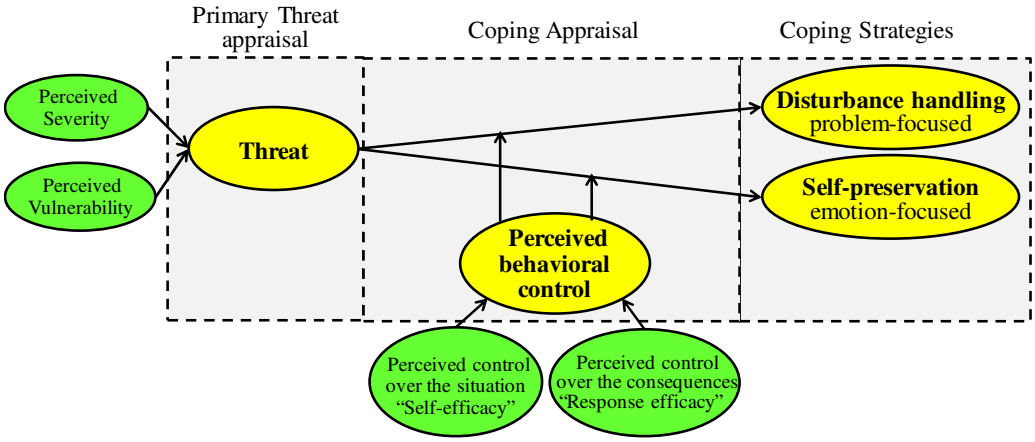


**Figure 23. Le CMUA complété avec les construits de la PMT (en vert) (AIM, 2019)**

Dans cette communication, nous montrons que la PMT permet d'expliquer de manière satisfaisante des stratégies centrées-émotion, légèrement moins bien toutefois que le CMUA. A l'inverse, le CMUA, bien qu'à l'origine non conçu pour étudier les comportements relatifs à la sécurité de l'information, se comporte de manière satisfaisante dans ce domaine : s'il vient après la PMT pour l'explication des comportements centrés-problème, il s'avère un très bon choix pour toute étude qui intègre à la fois la perception des opportunités, des menaces et traite à la fois de comportements centrés-problème et centrés-émotion.

Enfin, le CMUA me paraît prometteur pour étudier comment les problématiques de sécurité de l'information peuvent s'avérer génératrices de stress pour les dirigeants et décideurs, ceci représente un projet de recherche que j'escompte bien démarrer dès 2019-2020.

La partie suivante abandonne le cadre des théories du coping pour faire le point sur d'autres thèmes que j'ai étudiés dans le contexte de la SSI, mais aussi hors de ce contexte. Elle se termine par une proposition d'autres pistes potentielles d'encadrement doctoral.

## 2.2. Ouvertures vers d'autres thèmes, projets et encadrement doctoral

Cette section est composée de trois sous-sections. Premièrement, je présenterai les travaux qui n'ont pas mobilisé les théories du coping, mais toujours en lien avec la sécurité de l'information, soit respectivement les normes de sécurité et l'influence de l'expert-comptable sur le dirigeant de petite entreprise en matière de SI et de SSI. Deuxièmement, mes travaux sur l'évolution du rôle du DSI et deux thématiques qui ont donné lieu à l'encadrement de thésards, (1) l'impression 3D et l'innovation et (2) le big data et l'agilité organisationnelle. J'ouvrirai en conclusion de cette section mes travaux à des approches plus stratégiques et je proposerai des pistes d'encadrement de thésards.

### *2.2.1. Travaux en SSI 'hors coping'*

#### *2.2.1.1 Sécurité des S.I. et standardisation*

Parmi tous mes travaux, il s'agit du thème qui a généré le plus de citations sur Google Scholar, soit plus de 170 citations à ce jour. Ce thème correspond à la valorisation de certains de mes travaux préalables à la thèse : j'avais écrit plus d'une centaine de pages sur les normes de sécurité, qui ont été réduites à une dizaine de pages dans la thèse. En collaboration avec Vladislav Fomin, nous avons mis en parallèle l'adoption des normes ISO 9000 (qualité) et ISO 27001 (sécurité).

Ce travail a conduit à une communication présentée lors de l'Hawaii International Conference on System Sciences (HICSS) en 2008. Le titre de la communication était : « *Exploring the suitability of IS security management standards for SMEs* ». Dans un premier temps cette communication inventorie les similitudes puis les différences entre les deux normes. Ensuite, nous identifions les éléments qui vont favoriser et ceux qui peuvent limiter l'adoption de ISO 9000, toujours en comparaison avec ISO 27001. Ce travail conclut sur les possibilités de développer l'adoption de ISO 27001 par les entreprises. Notre principale suggestion est que le cadre législatif peut jouer un rôle crucial dans l'adoption des normes de sécurité.

Un troisième auteur, Henk de Vries, nous a rejoints pour une autre communication intitulée « *ISO/IEC 27001 Information Systems Security Management Standard: Exploring the Reasons for Low Adoption* » qui a été présentée à la conférence EuroMOT, toujours en 2008. Cette contribution ajoutait la norme environnementale ISO 14000 aux deux normes précédentes. L'analyse de l'historique de la diffusion de ces trois normes, aussi bien sur le plan de l'adoption par les entreprises que sur le plan des articles académiques et non-académiques publiés entre les années 1996 et 2006, a permis de mettre l'accent sur les facteurs qui nuisent à l'adoption de la norme de sécurité ISO 27001 et donc d'expliquer le faible succès de cette norme auprès des entreprises, notamment quant au nombre de certifications ISO 27001 accordées. Dans sa conclusion, cet article propose un ensemble de pistes pour de futures recherches.

Notre troisième contribution consiste en une revue de la littérature sur les normes de sécurité qui nous a permis de publier deux chapitres d'ouvrage en 2009 et 2010[21]. Ce travail s'intitule : « *The adoption of Information Security Management Standards: A Literature Review* ». Il présente les principales méthodes et normes de gestion de la sécurité de l'information utilisées dans le monde, en particulier les normes ISO 27001 et 27002. Il affine les travaux précédents afin de mieux comprendre les raisons du faible niveau d'adoption des normes de sécurité de l'information par les entreprises. Il identifie aussi les facteurs de succès de la mise en œuvre de ces normes. Sur la base des conclusions de la revue de la littérature, nous formulons des recommandations sur la manière de mettre en œuvre et de stimuler avec succès la diffusion des normes de sécurité de l'information dans un environnement commercial dynamique, avec une nécessité d'adaptation à des entreprises qui diffèrent principalement par leur taille et leur culture organisationnelle. Le chapitre se termine par une identification des évolutions nécessaires des normes de sécurité.

J'utilise toujours ces travaux dans le cadre de mes activités pédagogiques, ainsi que dans certaines recherches sur la SSI, afin de souligner leur impact dans le développement de la sécurité dans les entreprises. En effet, les normes de sécurité sont génératrices de comportements en SSI, notamment au sujet de dirigeants d'entreprises moyennes à grandes, plus susceptibles de mettre en place ces normes.

#### *2.2.1.2. La relation Dirigeant - Expert-comptable : impact sur le SI et la SSI*

Lors d'une présentation de ma thèse devant l'équipe de recherche MRM-SI en 2004, Robert Reix m'avait conseillé d'étudier la relation entre le dirigeant de très petite entreprise (TPE) et son expert-comptable (EC). Selon lui, l'EC pouvait exercer une forte influence sur les comportements des dirigeants en matière de protection des informations. Avec Annabelle Jaouen, nous avons décidé d'explorer cette relation dans le cadre d'une étude qualitative portant sur 10 entretiens avec des dirigeants de TPE et 12 EC.

[21] NB : il s'agit du même chapitre, qui a été repris par l'éditeur l'année suivante, dans un ouvrage différent.

Trois communications (AIM 2011, CIFEPME 2012, RENT 2012), ainsi qu'un chapitre d'ouvrage (2014) ont été tirés de cette étude. Il ressort de nos travaux d'une part le faible rôle joué par l'EC en matière de conseil en gestion de l'information, couplé à une méconnaissance des dirigeants de l'intérêt de recourir à ses services pour ces questions. D'autre part, les cabinets d'EC admettent ne pas développer ces prestations auprès de leurs clients. Pourquoi dans ce cas, le recours au conseil en gestion de l'information, essentiel pour l'entreprise et entrant pourtant dans le champ de compétences de l'EC, est-il si peu utilisé ? Plusieurs facteurs explicatifs ont été identifiés :

1. Le dirigeant a une image erronée du rôle de l'EC ;
2. Un comportement 'tendant à la facilité' de certains EC ne souhaitant pas développer ces prestations, par manque de temps essentiellement ;
3. Le fait que les dirigeants sont généralement en contact avec un collaborateur comptable qui n'a pas nécessairement les compétences nécessaires pour bien les conseiller ;
4. Le fait que les dirigeants semblent ne pas être informés lors de leur premier contact avec l'EC que ce ne sera plus leur interlocuteur privilégié par la suite.

Ceci aboutit à des divergences de perceptions et d'intérêts entre les deux types d'acteurs, qui ne facilitent pas cette relation de conseil. Le conseil en *gestion de l'information* entre l'EC et le dirigeant est peu formalisé (les missions sont au mieux 'balbutiantes'). Il est peu proactif du fait d'un attentisme de la sollicitation de la part des entreprises (qui, de plus, est faible). L'envergure de cette relation est souvent limitée, par exemple à la proposition d'achat d'un logiciel compatible ou à la facilitation des échanges d'informations EC-dirigeant. Cette relation de conseil est plus rare en cas de manque de compétences et/ou de temps de la part de l'EC, qui se cantonne alors à un rôle de "facilitateur", c'est-à-dire qu'il renvoie vers une personne compétente. En revanche, la relation de conseil en *sécurité de l'information* entre l'EC et le dirigeant est plus proactive, même si les missions sont aussi faiblement formalisées à ce jour. Elle se limite toutefois à des prestations de base : vérification des sauvegardes, conseils et informations sur les outils logiciels ou matériels de sécurité (sauvegardes, antivirus…), et parfois un envoi de courriers en cas de problèmes identifiés et non traités par l'entreprise (on peut se poser la question du bénéficiaire réel de cette démarche). Si nombre de dirigeants n'ont pas conscience de l'intérêt de protéger leurs informations, l'EC a un véritable rôle à jouer à ce niveau, en sensibilisant les dirigeants, en les conseillant sur quelques mesures basiques et en diffusant les bonnes pratiques à adopter. En conclusion, nous identifions des possibilités d'amélioration pour les experts-comptables, en communiquant plus avec les dirigeants et en étant plus proactifs. Enfin, les EC pourraient créer des missions formelles en gestion et en sécurité de l'information afin de proposer ces missions aux dirigeants d'entreprises.

Ces travaux restent aussi en phase avec les précédents, dans la mesure où je recherche les facteurs qui influencent les comportements des dirigeants. La piste des experts-comptables reste donc d'actualité et sera intégrée à l'une de mes prochaines études.

### *2.2.2. Travaux hors SSI et co-encadrement doctoral*

Mes travaux ne se limitent pas aux théories du coping et sortent du cadre de la sécurité de l'information. J'ai exploré d'autres champs de recherches tels que l'évolution du rôle du DSI, les technologies d'impression 3D et l'innovation et enfin les impacts des outils analytiques et du big data sur l'agilité organisationnelle et les stratégies d'innovation des entreprises.

*2.2.2.1. L'évolution du rôle du DSI*

Il s'agit d'un travail conceptuel qui a été présenté lors de la conférence AIM 2014 sous le titre : « *L'évolution du rôle du DSI : Etat de l'art et identification de pistes de recherche* ». La question de recherche traitée était : Quelles pistes de recherche peut-on identifier, afin de mieux comprendre et accompagner l'évolution du rôle du DSI ?

Cette communication traite de l'impact de facteurs récents tels que les réseaux sociaux, le big data, le cloud computing et les smartphones, sur le rôle du DSI. Après avoir réalisé un état de l'art concernant le rôle du DSI et les principales typologies identifiées dans la littérature académique, j'étudie les changements récents dans les comportements et les technologies, ainsi que leur impact sur le métier de DSI. J'ai identifié trois grands types d'évolutions du rôle du DSI :

- Une perte de pouvoir au profit des divers services de l'entreprise et des utilisateurs eux-mêmes ;
- Une réorientation marquée des préoccupations de la partie technologique vers la partie métier de l'entreprise, avec une nécessité de se tourner vers l'innovation, qu'elle soit dirigée vers l'intérieur ou l'extérieur (création de nouveaux produits et/ou services) de l'entreprise ;
- Une nécessité accrue d'accompagner et de tirer parti des évolutions récentes (cloud computing, réseaux sociaux et usages collaboratifs, Big Data, BYOD) tout en limitant les risques sur le plan de la sécurité de l'information (confidentialité et intégrité des données dans le cloud ou dans les équipements des salariés notamment).

Sur un plan théorique, les apports de ce travail résident dans l'analyse des typologies de DSI et dans les pistes identifiées pour de futures recherches. Sur un plan managérial, ce travail met en évidence la nécessité d'adopter une nouvelle gouvernance des SI, plus répartie entre les divers responsables de l'entreprise, la nécessité de gérer différemment les DSI, et enfin l'importance des technologies numériques, notamment dans l'amélioration de la relation avec les clients ainsi que dans la quête d'une plus grande agilité et d'une amélioration de la capacité d'innovation.

J'ai pour projet de soumettre à la revue IJIM une version mise à jour et complétée de ce travail, en adoptant une méthode de revue de littérature systématique (Templier et Paré, 2017).

*2.2.2.2. Impression 3D et Innovation (co-encadrement d'une thèse complète)*

Si ce thème correspond majoritairement au co-encadrement avec Florence Rodhain d'un thésard, Josip Maric, entre septembre 2013 et novembre 2018, date de soutenance de sa thèse, il correspond aussi à des travaux plus personnels et à des projets avec mon ex-thésard.

Cette recherche a pour but de répondre à deux questions principales portant sur la nature de l'impression 3D au niveau du consommateur et dans quelle mesure ces technologies d'impression 3D présentent des caractères relatifs à la durabilité et la responsabilité, et comment ces technologies vont-elles faciliter la durabilité et la responsabilité. Dans ce cadre, une étude qualitative a permis de mieux comprendre l'influence de la culture 'makers' sur l'adoption de l'impression 3D. Cette étude adopte une méthodologie basée sur la théorie ancrée (grounded theory) et des observations de type ethnographique. Quarante-quatre entretiens semi-directifs ont été conduits au sein des Fablabs et de la 'makers culture'. Ces entretiens sont complétés par 33 observations au sein de la Fablab de Montpellier en tant que membre de la communauté 'makers' locale, ainsi que par des données secondaires provenant de l'analyse des échanges en ligne entre les membres de la communauté 'makers' et des rapports divers. Le codage des données collectées lors des entretiens a permis d'identifier six catégories pour le thème « impression 3D » et trois catégories pour le thème 'makers'.

Les résultats mettent en avant les particularités de la culture Maker et des fablabs (espaces de coworking), la logique d'adoption, l'identification des utilisateurs précurseurs, les caractéristiques des fablabs et de l'impression 3DP dans un tel environnement. Les résultats mettent en évidence un déséquilibre entre les genres et éclairent le phénomène de la sous-représentation des femmes. Les technologies d'impression 3D présentent également un potentiel de changement radical pour le consommateur, illustré par le cas des prothèses imprimées en 3D. Les résultats informent aussi sur les tendances futures en matière d'adoption et de développement technologique. Une discussion s'ensuit au travers d'une triple approche concernant les implications sociales, économiques et environnementales détaillées de l'impression 3D au niveau du consommateur. Les impacts de ces technologies d'impression 3D sont ensuite remis en question.

Les apports théoriques sont doubles. Au niveau de l'impression 3D ce travail contribue aux théories sur la durabilité et l'impression 3D, sur l'adoption des technologies d'impression 3D au niveau du consommateur, ainsi que sur les espaces de coworking et les primo-utilisateurs. Au niveau de l'innovation responsable, ce travail de thèse contribue à l'enrichissement de la définition du concept d'innovation responsable et à sa mise en application au travers d'une recherche sur le terrain. Les apports managériaux sont pour les praticiens la proposition de stratégies commerciales pour mieux intégrer l'impression 3D, et des conseils sur l'alignement de l'impression 3D sur les activités existantes. Pour les institutions publiques il met en avant l'importance de mettre en place des politiques de financement public favorisant le développement de l'impression 3D, et les menaces relatives à cette technologie.

Cette thèse a donné lieu à la publication de deux articles dans des revues classées, un réalisé seul par le doctorant et un deuxième co-écrit avec Florence Rodhain (JIEM, 2016), intitulé « *Frugal innovations and 3D printing: insights from the field* » et publié dans le Journal of Innovation Economics and Management.

Pour la partie innovation en termes de pratiques, c'est-à-dire l'innovation managériale (Hamel, 2006), j'ai publié un chapitre d'ouvrage en 2013, intitulé « *Innovations managériales et S.I.* », faisant le point sur l'évolution des S.I. et des préoccupations des entreprises à ce sujet, des aspects stratégiques des S.I. et de leurs impacts sur les pratiques en entreprises au travers d'une présentation de trois cas pratiques portant sur les changements induits par le cloud computing et le SaaS, les logiciels libres et Linux, et enfin la mobilité et le m-commerce. Enfin, notre article présenté dans le 1.3.2.1 traite aussi des innovations managériales provoquées par le phénomène du BYOD (JOCM, 2018).

Ces thèmes liés à l'impression 3D et à l'innovation ont donné lieu à de nombreux projets de publications découlant notamment de la thèse. Voici les titres d'articles à venir, déjà présentés lors de conférences, qui devraient être soumis dans les prochains mois à des revues, toujours en collaboration avec Florence Rodhain et Josip Maric : « adoption logic with consumer-level 3DP and sustainability implications », « Open Innovation strategies and 3DP – case of the 3D-printed prostheses » et « Responsible innovation and the reverse logistics model ».

*2.2.2.3. Le Big Data et l'agilité (co-encadrement d'une année et 4 mois)*

Le thème du Big Data et des outils analytiques prend de plus en plus d'importance à mes yeux. J'ai présenté lors de la conférence MTO 2015 une communication intitulée « *Big Data et outils analytiques : incertitude et opportunités* ».

Faisant suite à ce travail, un article intitulé « *Big Data Analytics in turbulent contexts: Towards organizational change for enhanced agility* », co-écrit avec Paméla Baillette vient d'être accepté dans le cadre d'un numéro spécial de la revue Production Planning & Control (PPC, 2020). Cet article conceptuel est détaillé plus loin.

Mon intérêt pour ce thème m'a amené à co-encadrer une thésarde pendant un peu plus d'une année, entre octobre 2013 et janvier 2015, qui a malheureusement abandonné sa thèse à cause d'un 'éparpillement' trop important (montage d'une entreprise, présentations lors de conférences professionnelles, etc.). La doctorante était Myriam Criquet, et le co-encadrement a été réalisé avec Nathalie Mallet-Poujol[22] sur le thème des aspects juridiques du Big Data. Plus précisément, après une année de thèse elle évoquait sa vision de plus en plus complète de ce qu'est le Big Data, de son origine, de ses enjeux, des difficultés qu'il pose, tant en gestion qu'économiques, sociales, juridiques, philosophiques et géostratégiques. Elle devait se réinscrire en thèse et nous avait promis un plan et un début d'introduction pour février 2015. Elle n'a plus donné de nouvelles peu après.

L'article (PPC, 2020) est intitulé « *Big Data Analytics in turbulent contexts: Towards organizational change for enhanced agility* ». Il traite de la question de recherche suivante : *Quels types de changements organisationnels peuvent aider les entreprises à améliorer leur agilité pour prendre en compte les nouvelles capacités dynamiques offertes par les BDA[23] ?*

Cet article conceptuel traite des capacités offertes par les BDA, essentielles dans des environnements turbulents et dans le contexte de la « 4ième révolution industrielle ». Les BDA améliorent l'agilité organisationnelle (Tallon et Pinsonneault, 2011), car ils facilitent l'identification des opportunités et des menaces, c'est à dire le processus de détection ('sensing') de l'agilité (Côrte-Real *et al.*, 2017); toutefois, mis à part l'aide à la prise de décision que procurent les BDA, leurs apports dans le processus de réaction ('responding') sont plus difficiles à saisir sans adaptation organisationnelle. Par conséquent, les changements nécessaires pour exploiter pleinement les capacités offertes par les BDA, en particulier au niveau organisationnel, sont considérables. En adoptant une méthodologie d'analyse narrative de la littérature (Green *et al.*, 2006 ; Templier et Paré, 2018), cet article met en lumière plusieurs possibilités de changements organisationnels visant à développer l'agilité des entreprises et à tirer parti des BDA pour améliorer la performance et la position concurrentielle des entreprises dans des contextes turbulents. D'un point de vue théorique, cet article synthétise les principaux travaux académiques dans ce domaine et les rapproche des théories organisationnelles, telles que la knowledge-based view (KBV) et la resource-based view (RBV). D'un point de vue managérial, cette recherche propose plusieurs solutions pour améliorer les capacités de réaction des entreprises. L'article souligne également l'importance du rôle des dirigeants (le top management support ou TMS) dans la mise en place des changements nécessaires, ainsi que pour maximiser la valeur ajoutée apportée par les BDA afin d'accroître la position concurrentielle de l'entreprise. Enfin, de nombreuses pistes pour de futures recherches et/ou pour encadrer des doctorants sont proposées.

#### *2.2.2.4. Autres thématiques*

J'envisage d'étendre mes travaux à d'autres thématiques, en effet, dans mes activités pédagogiques, j'enseigne les aspects stratégiques des S.I. et le management stratégique de l'information, ce qui va constituer une première sous-partie. Mais, particulièrement aujourd'hui, les changements importants découlant de l'apparition de technologies 'disruptives' telles que le big data, le cloud computing ou encore les objets connectés, m'amènent à étudier l'improvisation et le bricolage organisationnel, qui feront l'objet de la seconde sous-partie.

[22] ERCIM, équipe CNRS, UMR 5885 Dynamique du droit.

[23] BDA : Big Data Analytics ou, en français, outils analytiques du big data.

*Stratégie et S.I.*

Un thème que je souhaite aussi développer à trait aux aspects stratégiques des S.I., j'assure d'ailleurs un cours spécifique sur ce thème, que j'enseigne depuis 2012, et cet intérêt m'a amené à présenter une communication à l'AIM en 2016, intitulé : « *Agilité organisationnelle et alignement stratégique : revue de la littérature et pistes de recherches* ».

Cette contribution, traite de la question de l'impact de l'agilité organisationnelle et de l'alignement stratégique T.I.-métiers sur la performance organisationnelle. Le discours est basé sur une revue de la littérature récente portant sur l'agilité et l'alignement, ainsi que sur l'interaction agilité-alignement. Il s'agissait ensuite de remonter aux modèles qui ont servi à étudier les déterminants de l'agilité et de l'alignement. Les modèles identifiés ont été regroupés dans un méta-modèle global, afin d'obtenir une vue d'ensemble des variables et de leurs déterminants, et ainsi mettre en évidence les concordances et divergences entre ces modèles.

Les apports théoriques de ce travail correspondent au méta-modèle conceptuel qui résume les principaux travaux identifiés, j'ai ensuite discuté ce méta-modèle afin d'identifier plusieurs pistes de recherches ou d'encadrement doctoral à développer dans le futur.

*Cloud computing : vers des stratégies d'échec rapide ?*

Ces aspects ont été publiés dans la revue MTO (Management des Technologies Organisationnelles) en 2015, dans un article intitulé « *Cloud computing et stratégie S.I.* » qui vise à répondre à la problématique suivante : « *Quels sont les impacts stratégiques du Cloud Computing sur les entreprises ?* ».

Cette contribution avait pour but de faire un point sur trois avantages stratégiques du cloud computing : (1) les opportunités stratégiques apportées aux PME et entreprises des pays émergents, (2) le développement de l'agilité et (3) de la capacité d'innovation organisationnelle. J'ai aussi relevé deux écueils, à savoir premièrement le danger de développement de silos fonctionnels et la nécessité d'adopter une gouvernance adaptée pour pallier ce problème, et deuxièmement les risques stratégiques liés à la transformation et aux changements dans les organisations, entrainés par le cloud computing, notamment ceux correspondant aux aspects humains.

Cet article introduit les stratégies d'échec rapide, basées sur de l'expérimentation et de l'improvisation, à coûts réduits grâce au cloud computing. Premièrement, l'expérimentation présente un intérêt stratégique puisqu'elle permet avant tout d'apprendre, qu'elle aboutisse à un succès ou un échec (McKeen et Smith, 2007). Deuxièmement, le cloud computing réduit très fortement les investissements liés à l'expérimentation, car il suffit de louer les infrastructures et applications nécessaires, et leur mise en place est simple et rapide. En conclusion, si l'on réussit, on en tirera les bénéfices, et si l'on échoue, non seulement on aura peu investi, en temps et en argent, mais surtout on apprendra de nos erreurs (McKeen et Smith, 2007). De plus, selon Venters et Whitley (2012), le cloud computing permet de réduire les cycles, de la mise à disposition à l'utilisation effective, de quelques semaines (voire des mois) à quelques jours, ce qui va se traduire en opportunités métiers, qui peuvent conduire à un avantage concurrentiel. On peut donc réduire le temps d'innovation et de mise sur le marché des innovations (Venters et Whitley, 2012). On pourra ainsi lancer de nouveaux produits et services, ou entrer sur de nouveaux segments de marché (Roberts et Grover, 2012). L'expérimentation peut aller jusqu'à l'improvisation (Weick, 1993) ou le bricolage (Ciborra, 2002), tout en conservant un aspect stratégique (Moorman et Miner, 1998).

S'il facilite les stratégies d'expérimentation et d'improvisation, le cloud computing permet d'aller encore plus loin : certains parlent "*d'échec rapide*" (Bils, 2011). A ce sujet, McQuivey

(2013) souligne que les DSI "*échouent, habituellement plus fréquemment qu'ils ne réussissent, mais comme ils exploitent des plateformes numériques qui ne requièrent quasiment aucun investissement et apportent un retour d'expérience presque immédiat, on peut apprendre de l'échec à un coût réduit*". Et selon Beckler (2013), "*le but est d'échouer rapidement plutôt que de laisser de mauvaises idées prendre du temps à notre service développement […], pour faire ceci, nous amenons un maximum d'idées face à nos clients aussi fréquemment que possible, sans investir énormément dans aucune d'elle, sans preuve de leur valeur*". Les pertes potentielles liées à l'échec sont donc suffisamment faibles pour que l'apprentissage organisationnel à partir des erreurs puisse compenser ces pertes, voire renverser la balance. L'important est de conserver une certaine autorégulation afin d'éviter des excès et s'assurer que l'apprentissage à partir des erreurs reste effectif (Ferneley et Bell, 2006 ; Gong *et al.*, 2019).

Les impacts des spécificités du cloud computing (investissements faibles et facilité/rapidité de mise en œuvre) sur les stratégies d'entreprises méritent plus de travaux académiques. De même, l'improvisation et le bricolage organisationnel pourraient être explorés plus en profondeur dans le contexte du cloud computing. Enfin, une mise en perspective des stratégies d'échec rapide vis-à-vis des stratégies plus classiques me semble un sujet très intéressant. Ces éléments constituent pour moi des pistes d'encadrements de thèses.

## 2.3. Conclusion et proposition de pistes d'encadrement de doctorants

Si j'ai déjà co-encadré deux doctorants, Josip Maric (impression 3D et innovation) et Myriam Criquet (problématiques relatives au Big Data), je souhaite aller plus loin dans ce travail d'encadrement grâce à une HDR, afin de co-diriger voire de diriger seul des doctorants. Dans ce contexte, je propose plusieurs programmes de recherches pouvant se décliner en travaux doctoraux :

1. Les théories du coping : prolongement et validation via des études quantitatives ;
2. Les comportements relatifs à la SSI et leurs déterminants vis-à-vis de technologies et concepts récents tels que l'internet des objets, la shadow IT et les problématiques posées par le Big Data : Ici, des « mixed methods » ou des méthodologies plus qualitatives peuvent être envisagées ;
3. Des programmes correspondant à l'ouverture des problématiques de la SSI à des considérations plus larges, ayant des implications éthiques voire philosophiques, seront proposés dans la conclusion générale.

*Le premier programme de recherches* correspond à mes travaux sur les théories du coping. Les pistes correspondantes sont majoritairement orientées vers l'étude des comportements des acteurs, employés, managers et dirigeants, en mobilisant les théories comportementales du coping dans le contexte de la SSI, par le biais de méthodologies majoritairement quantitatives. Dans cette optique, voici quelques problématiques et des exemples de thèmes qui pourraient être approfondis par des doctorants. Dans un premier temps, les études quantitatives se sont surtout focalisées sur des comportements centrés-problème, alors que le but principal des théories du coping (voir figure 4) est d'aboutir à un 'rééquilibrage émotionnel'. Il est donc important, tant sur un plan théorique que managérial, de s'intéresser à ces stratégies centrées-émotion, en plus de celles centrées-problème. Des travaux dans ce domaine permettraient non seulement d'obtenir un nouvel éclairage sur ces comportements, mais aussi de conseiller les acteurs en entreprise pour mieux gérer la SSI de leur entreprise.

Voici quelques exemples de travaux :

- Les comportements centré-problème et centrés-émotion relatifs à la sécurité des S.I : adaptations et compléments des échelles du WOCC (ways of coping checklist) de Lazarus et Folkman (1984) et le rattachement de ces échelles aux diverses stratégies de coping ;
- Utilisation de la PMT pour étudier des comportements centrés-émotion ; comparaison de son pouvoir explicatif comparé à des comportements centrés-problème ;
- Le technostress relatif aux stratégies centrées-émotion en SSI, autrement dit « *Je n'agis pas pour me protéger, du coup cela me stresse* ». Les contextes peuvent être privés ou professionnels.

Il est aussi possible d'aller au-delà des comportements étudiés jusqu'à présent en SSI, (c'est-à-dire mettre en place des protections, ne rien faire ou encore avoir des comportements déviants) en s'intéressant aux risques générés par l'introduction de technologies récentes en entreprise. Les questions sous-jacentes sont : vais-je accepter ou non d'introduire une technologie présentant des risques ? Le CMUA apparait comme un modèle très intéressant pour étudier comment s'équilibrent les aspects positifs de ces technologies, mais aussi les risques qu'elles peuvent provoquer. En poussant plus loin ce raisonnement, il serait possible d'étudier l'apparition de paradoxes du type : je suis très préoccupé par les risques posés par cette technologie, je ne sais pas me protéger (ou protéger mon entreprise), pourtant je l'introduis malgré tout car je sur-priorise ses aspects positifs. Nous avons commencé à étudier ces aspects dans l'article JGIM (2020). Sur un plan managérial, les implications sont évidentes quand il s'agit de limiter les risques encourus par les salariés (au sujet de leur vie privée) et les dirigeants (au sujet des informations de leur entreprise).

- Etude des opportunités et menaces en termes de SSI représentées par l'introduction (par les dirigeants) ou l'usage (par les salariés et individus) de diverses technologies telles que des objets connectés, des applications en cloud computing (SaaS), des réseaux sociaux professionnels ;
- Les paradoxes en sécurité de l'information ou plus spécifiquement les 'privacy paradoxes'. Application à divers contextes d'adoption inversée ou d'adoption de technologies invasives à titre privé ;
- Adoption inversée de technologies et/ou Shadow IT en entreprise et perception des risques : vers un chaos en SSI ?

Enfin, les dirigeants de PME méritent d'être plus étudiés, nous avons montré (SIM, 2019) que les déterminants du soutien du dirigeant, pourtant d'une très grande importance dans l'amélioration de la SSI des entreprises, méritaient d'être examinés en profondeur. De plus, les dirigeants n'ont pas les mêmes motivations que les salariés dans l'adoption de mesures de sécurité, et subissent des pressions différentes. Par exemple la théorie générale de la dissuasion est moins pertinente pour les dirigeants que pour les salariés, à l'inverse, les dirigeants vont subir des pressions provenant des règlementations ou de leurs pairs et partenaires, qui vont différer de celles auxquelles sont soumis les employés. Voici trois thèmes ci-dessous ayant pour but d'approfondir ces réflexions.

- L'impact du soutien du dirigeant (Top Management Support) sur les comportements en SSI des salariés d'entreprises ;
- Enrichissement des modèles du coping avec la théorie des liens sociaux , la théorie néo-institutionnelle dans le contexte de la SSI ;
- Mobilisation de la théorie néo-institutionnelle pour l'amélioration de la SSI en entreprise. Dans ce contexte, le rôle de la norme ISO 27000 et ses limites (lacunes, guides, mise en place, etc.) pourrait par exemple être étudié.

Ces thèmes pourront être déclinés dans des contextes tels que les différents types de dirigeants de PME (propriétaires ou non, entreprises familiales ou non), impact des générations (X, Y et Z) sur l'appréciation des dangers et la mise en place de mesures en SSI, etc.

*Le deuxième programme de recherches* que je propose d'encadrer a pour but d'ouvrir les comportements relatifs à la SSI aux effets des interactions entre les divers acteurs internes et externes, et à d'autres facteurs de motivation et de démotivation à l'adoption de comportements en SSI. Dans ma thèse (2001-2006), j'avais adopté un positionnement interprétativiste et utilisé une méthodologie qualitative basée sur des entretiens semi-directifs, ce qui m'avait permis d'identifier une palette riche de comportements (dirigeants, DSI et employés) et certains comportements inattendus (les 'salariés-RSSI'). Mes travaux sur les experts-comptables (2011) étaient aussi basés sur ce type d'approche et enfin, la thèse de mon doctorant Josip Maric (2018) était basée sur une théorie enracinée. Il n'est donc pas exclu que je prenne la direction de doctorants dans le cadre de méthodes plus qualitatives, afin de faire émerger de nouvelles hypothèses à partir du terrain. Des méthodes de type « mixed-method » (Annansingh et Howell, 2016 ; Venkatesh *et al.*, 2013) pourraient s'avérer un bon compromis car elles font appel à des approches qualitatives et quantitatives soit simultanément (c.-à-d. indépendantes les unes des autres), soit séquentiellement (les résultats d'une approche éclairent l'autre approche), pour comprendre un phénomène.

La première piste fait suite aux travaux sur l'influence de l'entourage du dirigeant. Afin d'améliorer l'impact des avis et conseils sur les initiatives des dirigeants d'amélioration de la SSI de leur entreprise, il convient d'approfondir plusieurs éléments :

- Le rôle de l'entourage des dirigeants de PME dans le déclenchement des actions en SSI : Quels types d'acteurs ? Quels facteurs ? Lesquels ont plus d'influence que d'autres ?

Dans ma thèse, j'avais identifié l'apparition d'un poste informel de 'salarié-RSSI', qui jouait un rôle important dans l'amélioration de la SSI en PME. De nombreux travaux sont encore nécessaires pour mieux comprendre comme cette fonction apparait, et surtout comment faciliter la tâche mais aussi d'améliorer l'influence de ces salariés-RSSI sur les employés et dirigeants de leur entreprise :

- Les salariés-RSSI : quels profils ? comment améliorer leur motivation, leur crédibilité, leur influence sur les dirigeants de PME ? sur leurs collègues ? sur la SSI de l'entreprise ?

Les dirigeants de PME sont parfois seuls lorsqu'il s'agit de prendre en charge la SSI de leur entreprise, cela peut par exemple être le cas dans les plus petites entreprises. Il s'avère donc important de mieux comprendre dans ce contexte quels sont leurs comportements face à la SSI. La piste suivante pourrait apporter un éclairage sur les processus décisionnels des dirigeants :

- Dirigeants de PME et SSI : La part des stratégies raisonnées et des comportements de bricolage organisationnel et d'effectuation dans la mise en place de mesures de SSI et leur impact sur la protection des entreprises.

# Conclusion générale

Ce travail d'habilitation à diriger des recherches témoigne de ma transition progressive de la pédagogie vers la recherche : cela fait maintenant trente années que je suis enseignant, et mes activités de recherche ont débuté en 2001. Mais surtout, ce document réalise un bilan des treize années qui ont suivi l'obtention de mon doctorat en décembre 2006. Ce mémoire établit un lien entre mes principaux travaux au travers des théories du coping et ouvre de nombreuses perspectives pour de futurs travaux. J'ai développé ma réflexion sur ces théories à partir des travaux originels de Lazarus (1966), puis de la théorie de la motivation à la protection de Rogers (1983) pour terminer par le coping model of user adaptation de Beaudry et Pinsonneault (2005). Après avoir mis en lumière les possibilités d'enrichissement de ces modèles dans le cadre de l'explication des comportements relatifs à la sécurité des informations, j'ai examiné comment compléter ces théories, non seulement pour augmenter le pouvoir explicatif de ces modèles, mais aussi pour expliquer d'autres types de comportements relatifs à la SSI, tels que les comportements de soutien des dirigeants ou encore certains comportements centrés-émotion. Toutes ces pistes d'enrichissement pourront devenir la source de nouveaux projets d'encadrement de doctorants originaux.

Toutefois, les programmes de recherche proposés n'ont pas prétention à être exhaustifs car de nombreuses questions restent à explorer dans le contexte de la SSI. Historiquement, la SSI était avant tout technique, ce qui se traduisait par des normes tout aussi techniques, comme on peut le voir dans les premières normes, telles que les ITSEC ou les 'critères communs', datant du milieu des années 1990. Puis le facteur humain a été progressivement introduit. Toutefois, la sécurité restait avant tout une histoire d'obligations que l'on devait respecter sous peine de sanctions, preuve en est la théorie générale de la dissuasion de Straub et Welke (1998). La sécurité était aussi un prérequis pour pérenniser le fonctionnement de l'entreprise, représentant avant tout un coût (Maslow, 1954 ; Urwiler et Frolick, 2008). Mais cette sécurité vécue comme une contrainte a continué d'évoluer pour être peu à peu perçue comme une source de profits et son ROSI (return on security investments) a été envisagé (Drugescu et Etges, 2008). Les aspects humains ont été pris en compte de manière plus positive, intégrant par exemple l'habitude (Limayem et Hirt, 2003 ; 2007), ou des facteurs d'attachement à l'entreprise comme des facteurs bénéfiques pour l'adoption de comportements en SSI. D'où la nécessité, pour les managers, de considérer autrement la sécurité.

La sécurité de l'information peut-elle encore aujourd'hui être réduite à « l'inverse du risque » ? Ne doit-elle pas, pour être correctement gérée, être un vecteur de développement personnel ? Les comportements relatifs à la SSI sont-ils des routines (Polites et Karahanna, 2013) ou des processus récursifs en amélioration continue ? Même si le CMUA intègre un processus récursif d'appréciation-réappréciation d'une menace, n'est-il pas nécessaire de réfléchir à une nouvelle conceptualisation des comportements en SSI ?

Dans une vision plus large encore, d'autres pistes de recherche peuvent être envisagées, notamment en s'interrogeant sur la dimension éthique de la SSI. En effet, les informations personnelles sont de plus en plus numérisées, qu'elles soient à but 'utilitaire' (factures, relevés, documents administratifs) ou dans une optique de loisirs (images, conversations, traces de nos achats et voyages). Leur perte peut non seulement nous affecter, mais leur divulgation va directement porter atteinte à notre vie privée. A ce sujet, des technologies de plus en plus intrusives et polymorphes apparaissent, posant des problèmes majeurs. A titre d'exemple, le système chinois de points sociaux, dont l'attribution et le retrait est basé sur un contrôle quasi permanent des individus, grâce à des intelligences artificielles qui vont interpréter notamment les images de caméras de contrôle. Sans aller si loin, nos outils personnels, que ce soit un ordinateur portable, un smartphone, voire une simple télévision connectée peuvent enregistrer

les images, les sons de notre vie privée. Des hackers ou des sociétés de marketing (cela s'est déjà produit par le biais de logiciels espions intégrés aux TV sur le territoire américain) peuvent exploiter ces données pour des raisons contestables, voire carrément illégales. De la même manière, les informations sont elles-mêmes stockées soit localement, soit dans des endroits qui nous échappent totalement, que ce soit dans les bases de données de réseaux sociaux ou encore dans les 'clouds' des opérateurs de téléphonie (Orange, Free, etc.) ou des fournisseurs de matériels (Apple, Huawei, Samsung, etc.). Dès lors, quels comportements les individus peuvent-ils adopter, s'ils ne sont même pas conscients des risques encourus ou des moyens de se protéger ? Quels comportements non-éthiques ou déviants peuvent apparaître ? Dans certains contextes, les fondamentaux mêmes des modèles basés sur le coping pourront être remis en question quand il s'agira d'étudier ces comportements émergents.

Nous avons abordé la collecte et l'analyse des données ci-dessus, mais les outils analytiques du big data posent aussi des problèmes (MTO 2012 ; MTO, 2015 ; AIM, 2018). Du fait des corrélations (lieux, habitudes, achats, temporalité, etc.), l'anonymat n'existe virtuellement plus. Les intelligences artificielles derrière ces outils peuvent non-seulement violer notre vie privée, mais parfois aller jusqu'à remettre notre propre vie en question ! A titre d'exemple, la voiture autonome qui a considéré une cycliste comme un faux positif et n'a pas ralenti pour préserver le confort de son passager… Les robots, basés eux aussi sur des intelligences artificielles, commencent également à coopérer et à négocier des transactions à la place des humains. Devront-ils également apprendre à développer des comportements relatifs à la SSI ?

Quels modèles, quelles méthodologies pourront permettre l'étude de ces nouvelles problématiques ?

Ceci constitue des pistes de recherche dont la portée économique et sociétale est majeure. Le débat est donc loin d'être clos…

# Bibliographie


Ajzen, I. (1991), The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes*, vol. 50, n°2, p. 179-211.

Ament, C., & Haag, S. (2016), Security-Related Stress - A Neglected Construct in Information Systems Stress Literature. *European Conference on Information Systems (ECIS)*, Istanbul, Turkey, June 12-15, paper 74.

Anderson, C.L., & Agarwal, R. (2010), Practicing Safe Computing: a Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly*, vol. 34, n°3, p. 613-644.

Angst, C.M., Block, E.S., D'Arcy, J., & Kelley, K. (2017), When do IT Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches. *MIS Quarterly*, vol. 41, n°3, p. 893-916.

Aurigemma, S., & Mattson, T. (2018), Exploring the effect of uncertainty avoidance on taking voluntary protective security actions, *Computers & Security*, vol.73, p. 219–234.

Annansingh, F., & Howell, K. (2016), Using Phenomenological Constructivism to Discuss a Mixed Method Approach in Information Systems Research. *The Electronic Journal of Business Research Methods*, vol. 14, n°1, p. 39-49.

Avolio, F.M. (2000), Best practices in network security: as the networking landscape changes, so must the policies that govern its use. Don't be afraid of imperfection when it comes to developing those for your group. *Network Computing*, vol. 60, n°20, p. 60-72.

Ayyagari, R., Grover, V., & Purvis, R. (2011), Technostress: Technological Antecedents and Implications. *MIS Quarterly*, vol. 35 n°4, p. 831-858.

Bandura, A. (1977), Self-efficacy: Toward a Unifying Theory of Behavioral Change. *Psychological Review,* vol. 84, n°3, p. 191-215.

Bandura, A. (1994), "Self-efficacy" in *Encyclopedia of Human Behavior*, V.S. Ramachandran (Ed), Academic Press, New York, NY, p. 71-81.

Beaudry, A., & Pinsonneault, A. (2005), Understanding user responses to information technology: A coping model of user adaptation. *MIS Quarterly*, vol. 29, n°3, p. 493-524.

Beaudry, A., & Pinsonneault, A. (2010), The other side of acceptance: Studying the direct and indirect effects of emotions on information technology use. *MIS Quarterly*, vol. 34, n°4, p. 689-710.

Beckler, B. (2013), 'Failing fast' is the best way to discover what works for IT users. *ComputerWeekly*, 23 April, p. 11-12.

Benlian, A., & Hess, T. (2011), Opportunities and risks of software-as-a-service: Findings from a survey of IT executives. *Decision Support Systems*, vol. 52, n°1, p. 232-246.

Bérard, E., Flachère, I., Saulpic, O., & Zarlowski, P. (2015), Les outils financiers dans les hôpitaux : penser leur déploiement au-delà de la dimension technique. *Journal de gestion et d'économie médicales*, vol. 33, n°7, p. 409-427.

Bharadwaj, A., El Sawi, O.A., Pavlou, P.A., & Venkatraman, N. (2013), Digital Business Strategy: Toward a Next Generation of Insights. *MIS Quarterly,* vol. 37, n°2, p. 471-482.

Bhattacherjee, A., Davis, C.J., Connolly, A.J., & Hikmet, N. (2018), User response to mandatory IT use: A Coping Theory perspective. *European Journal of Information Systems*, vol. 27, n°4, p. 395-414.

Birkinshaw, J., & Mol M.J. (2006), How Management Innovation Happens. *Sloan Management Review*, vol. 47, n°4, p. 81-88.

Boonstra, A. (2013), How do Top Managers Support Strategic Information System Projects and Why do they Sometimes Withhold this Support? *International Journal of Project Management*, vol. 31, n°3, p. 498-512.

Boss, S. R., Galletta D. F., Lowry P. B., Moody G. D., & Polak P. (2015), What do Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors. *MIS Quarterly*, vol. 39, n°3, p. 837-864.

Bourret, R., Martinez, E., Vert, M., Vernhet, A., Naro, G. (2013), La certification des comptes des hôpitaux publics à l'horizon 2014 : un état de l'art au travers du témoignage du CHRU de Montpellier. *Politiques et Management Public*, vol. 30, n°4, p. 571-581.

Carver, C. S., Scheier, M. F., & Weintraub, J. K. (1989), Assessing coping strategies: A theoretically based approach. *Journal of Personality and Social Psychology*, vol. 56, p. 267-283.

Cavusoglu, H., Cavusoglu, H., Son, J.-Y., & Benbasat, I. (2015), Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. *Information & Management*, vol. 52, p. 385-400.

Chandon, P., Morwitz, V.G., & Reinartz, W.J. (2005), Do Intentions Really Predict Behavior? Self-Generated Validity Effects in Survey Research. *Journal of Marketing,* vol. 69, p. 1-14.

Chen, Y., & Zahedi F. M. (2016), Individuals' internet Security Perceptions and Behaviors: Polycontextual Contrasts between the United States and China. *MIS Quarterly*, vol. 40, n°3, p. 205–222.

Cheng, L., Li, Y., Li., W., Holm, E., Zhai, Q. (2013), Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security*, vol. 39, part B, p. 447-459.

Ciborra, C. (2002), *The labyrinths of information: challenging the wisdom of systems*. Oxford University Press, Oxford.

Cigref. (2013), *La contribution de l'IT à l'innovation*, juin, 22p.

Clusif. (2018), *Menaces informatiques et pratiques de sécurité en France*. Accédé le 15/03/2019, https://clusif.fr/publications/menaces-informatiques-pratiques-de-securite-france-edition-2018-rapport/

Côrte-Real, N., Oliveira, T., & Ruivo, P. (2017), Assessing business value of Big Data Analytics in European firms. *Journal of Business Research*, vol. 70, p. 379-390.

Cram, W.A., D'Arcy, J., & Proudfoot, J.G. (2019), Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance. *MIS Quarterly*, vol. 43, n°2, p. 525-554.

Crossler, R.E, Andoh-Baidoo, F.K., & Menard, P. (2019), Espoused cultural values as antecedents of individuals' threat and coping appraisal toward protective information technologies: Study of U.S. and Ghana. *Information & Management*, 56, p. 754–766.

Crossler, R.E., & Bélanger F. (2014), An Extended Perspective on Individual Security Behaviors. *SIGMIS Database*, vol. 45, n°3, p. 51-71.

Crossler, R.E., Johnston, A.C., Lowry P.B., Hu Q., Warkentin, M., & Baskerville, R. (2013), Future directions for behavioral information security research. *Computers & Security*, vol. 32, n°1, p. 90-101.

Crossler, R.E., Long, J.H., Loraas, T.M., & Trinkle, B.S. (2014), Understanding Compliance with Bring Your Own Device Policies Utilizing Protection Motivation Theory: Bridging the Intention-Behavior Gap. *Journal of Information Systems*, vol. 28, n°1, p. 209-226.

Daud, M., Rasiah, R., George, M., Asirvatham, D., & Thangiah, G. (2018), Bridging the Gap between Organisational Practices and Cyber Security Compliance: Can Cooperation Promote Compliance in Organisations?. *International Journal of Business & Society*, vol. 19, n°3, p. 161-180.

Davis, F.D. (1986), *Technology acceptance model for empirically testing new end user information sytems theory and results*. Thèse de doctorat non publiée, MIT.

Davis, F.D. (1989), Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, vol. 13, n°3, p. 319-339.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989), User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Management Science*, vol. 35, n°8, p. 982-1002.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1992), Extrinsic and Intrinsic Motivation to Use Computers in the Workplace. *Journal of Applied Social Psychology*, vol. 22, n°14, p. 1111-1132.

D'Arcy, J., & Herath, T. (2011), A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems*, vol. 20, p. 643-658.

D'Arcy, J., Herath, T., & Shoss, M. (2014), Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of Management Information Systems*, vol. 31, n°2, p. 285-318.

D'Arcy, J., Hovav, A., & Galletta, D.F. (2009), User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research,* vol. 23, n°1, p. 79-98.

De Kok, A., Lubbers, Y., & Helms, R.W. (2015), Mobility and Security in the New Way of Working: Employee Satisfaction in a Choose Your Own Device (CYOD) Environment. *9th Mediterranean Conference on Information Systems*, Greece, 73-92.

Deci, E.L. (1975), *Intrinsic Motivation*. Plenum press, NY, USA.

Deci, E.L., & Ryan, R.M. (1985), *Intrinsic motivation and self-determination in human behavior*. Plenum Press, NY, 371p.

DiMaggio, P.J., & Powell, W.W. (1983), Iron cage revisited: institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, vol. 48, n°2, p. 147-160.

Djellal, F. (2014), Les logiques d'innovation à l'hôpital. *Revue Soins cadres,* vol. 91, p. 16-20.

Dong, L., Neufeld, D., & Higgins, C. (2009), Top management support of enterprise systems implementations. *Journal of Information Technology*, n°24, p. 55-80.

Drugescu, C., & Etges, R. (2008), Maximizing the return on investment of information security programs: program governance and metrics. *Information systems security*, December, p. 30-40.

Elie-Dit-Cosaque, C.M., & Straub, D.W. (2011), Opening the black box of system usage: User adaptation to disruptive IT. *European Journal of Information Systems*, vol. 20, n°5, p. 589-607.

Fayolle, A., Barbosa, S.D., & Kickul, J. (2008), Une nouvelle approche du risque en création d'entreprise. *Revue Française de Gestion*, vol. 185, p. 141-159.

Feng, G., Zhu, J. Wang, N., & Liang, H. (2019), How Paternalistic Leadership Influences IT Security Policy Compliance: The Mediating Role of the Social Bond, *Journal of the Association for Information Systems*, vol. 20, n°11, p. 1650-1691.

Ferneley, E., & Bell, F. (2006), Using bricolage to integrate business and information technology innovation in SMEs. *Technovation*, vol. 26, p. 232-241.

Fishbein, M., & Ajzen, I. (1975), *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*. Addison-Wesley, Reading, MA.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000), A Meta-Analysis of Research on Protection Motivation Theory. *Journal of Applied Social Psychology*, vol. 30, n°3, p. 407-429.

Folkman, S. (1992), Making the case for coping. In B. N. Carpenter (Ed.), *Personal coping: Theory, research, and application* (p. 31-46). Westport, CT: Praeger.

Folkman, S., Lazarus, R. S., Gruen, R. J., & DeLongis, A. (1986), Appraisal, coping, health status, and psychological symptoms. *Journal of Personality and Social Psychology*, vol. 50, n°3, p. 571-579.

Folkman, S., Lazarus, R. S. (1988), *Manual for the Ways of Coping Questionnaire*. Palo Alto, CA, Consulting Psychologists Press.

Friend, M., & Pagliari, L.R. (2000), Establishing a safety culture: getting started. *Professional Safety*, vol. 45, n°5, p. 30-32.

Gong, Y., Zhang, Y., & Xia, J. (2019), Do Firms Learn More from Small or Big Successes and Failures? A Test of the Outcome-Based Feedback Learning Perspective. *Journal of Management*, vol. 45, n°3, p. 1034-1056.

Gottfredson, M.R., & Hirschi, T.A. (1990), *A General Theory of crime*. Stanford University Press, CA, 297p.

Gottschalk, P. (1999), Strategic Information Systems Planning: the IT Strategy Implementation Matrix. *European Journal of Information Systems*, vol. 8, n°3, p. 107-118.

Green, B.N., Johnson, C.D., & Adams, A. (2006), Writing narrative literature reviews for peer-review journals: Secrets of the trade. *Journal of Chiropractic Medicine*, vol. 5, p. 101-117.

Grimes, M., & Marquardson, J. (2019), Quality matters: Evoking subjective norms and coping appraisals by system design to increase security intentions. *Decision Support Systems*, 119, p. 23-34.

Gupta, A., & Hammond, R. (2005), Information systems security issues and decisions for small businesses: an empirical examination. *Information Management and Computer Security*, vol. 13, n°4, p. 297-310.

Gurung, A., Luo, X., & Liao, Q. (2009), Consumer Motivations in Taking Action Against Spyware: An Empirical Investigation. *Information Management & Computer Security*, vol. 17, n°3, p. 276-289.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011), PLS-SEM: Indeed a Silver Bullet. *The Journal of Marketing Theory and Practice*, vol. 19, n°3, p. 139-152.

Hair, J. F., Sarstedt, M., & Ringle, C. M. (2019), Rethinking some of the rethinking of partial least squares", *European Journal of Marketing*, vol. 53, n°4, p. 566-584.

Hamel, G. (2006), The Why, What, and How of Management Innovation. *Harvard Business Review*, vol. 84, n°2, p. 1-16.

Hanus, B., & Wu, Y. A. (2016), Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *Information Systems Management*, vol. 33, n°3, p. 2-16.

Harris, J.G., Ives, B., & Junglas, I. (2012), IT consumerization: When gadgets turn into enterprise IT tools. *MIS Quarterly Executive*, vol. 11, n°3, p. 99-112.

Herath, T., & Rao, H.R. (2009), Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness. *Decision Support Systems,* vol. 47, n°2, p. 154-165.

Hina, S., Panneer Selvam, D.D.D., & Lowry, P.B. (2019), Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. *Computers & Security*, vol. 87.

Hovav, A., & D'Arcy, J. (2012), Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. *Information & Management*, vol. 49, p. 99-110.

Hovav, A., & Putri, F. F. (2016), This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy. *Pervasive and Mobile Computing*, vol. 32, p. 35-49.

Hu, Q., Hart, P., & Cooke, D. (2007), The role of external and internal influences on information systems security – a neo-institutional perspective. *Journal of Strategic Information Systems*, vol. 16, p. 153-172.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012), Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. *Decision Sciences*, vol. 43, n°3, p. 615-660.

Hu, Q., Xu, Z.H., Dinev, T., & Ling, H. (2011), Does Deterrence Work in Reducing Information Security Policy Abuse by Employees? *Communications of the ACM*, vol. 54, n°6, p. 54-60.

Hwang, I., & Cha, O. (2018), Examining technostress creators and role stress as potential threats to employees' information security compliance. *Computers in Human Behavior*, vol.81, p. 282-293.

Ifinedo, P. (2012), Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory. *Computers & Security,* vol. 31, n°1, p. 83-95.

Ifinedo, P. (2014), Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, vol. 51, p. 69-79.

Indihar Štemberger, M., Manfreda, A., & Kovačič, A. (2011), Achieving Top Management Support with Business Knowledge and Role of IT/IS Personnel. *International Journal of Information Management*, vol. 31, n°3, p. 428-436.

Jansen, J., & van Schaik, P. (2018), Testing a model of precautionary online behaviour: The case of online Banking. *Computers in Human Behavior*, vol. 87, p. 371-383.

Jarvenpaa, S. L., & Ives, B. (1991), Executive Involvement and Participation in the Management of Information Technology. *MIS Quarterly*, vol. 15, n°3, p. 205-227.

Jenkins, P.H. (1997), School delinquency and the school social bond. *Journal of Research in Crime and Delinquency*, vol. 34, n°3, p. 337-367.

Johnston, A. C., & Hale, R. (2009), Improved Security through Information Security Governance. *Communications of the ACM*, vol. 52, n°1, p. 126-129.

Johnston, A. C., & Warkentin, M. (2010), Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly*, vol. 34, n°3, p. 549-566.

Johnston, A. C., Warkentin, M., & Siponen, M. T. (2015), An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric. *MIS Quarterly*, vol. 39, n°3, p. 113-134.

Kankanhalli, A., Teo, H.-H., Tan, B.C., & Wei, K.-K. (2003), An Integrative Study of Information Systems Security Effectiveness. *International Journal of Information Management,* vol. 23, n°2, p. 139-154.

Karimi, J., & Walter, Z. (2015), The Role of Dynamic Capabilities in Responding to Digital Disruption: A Factor-Based Study of the Newspaper Industry. *Journal of Management Information Systems*, vol. 32, n°1, p. 39-81.

Keith, M.J., Thompson, S.C., Hale, J., Lowry, P.B., & Greer, C. (2013), Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human Computer Studies*, vol. 71, n°12, p. 1163-1173.

Kim, Y. H., Kim, D. J., & Wachter, K. (2013), A study of mobile user engagement (MoEN): Engagement motivations, perceived value, satisfaction, and continued engagement intention. *Decision Support Systems,* vol. 56, p. 361-370.

Klein, H.K., & Myers, M.D. (1999), A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems. *MIS Quarterly*, vol. 23, n°1, p. 67-94.

Kulkarni, U., Robles-Flores, J., & Popovič, A. (2017), Business Intelligence Capability: The Effect of Top Management and the Mediating Roles of User Participation and Analytical Decision-Making Orientation. *Journal of the Association for Information Systems*, vol. 18, n°3, p. 516-541.

Law, C. C. H., & Ngai, E. W. T. (2007), ERP systems adoption: An exploratory study of the organizational factors and impacts of ERP success. *Information & Management*, vol. 44, n°4, p. 418-432.

Lazarus, R.S. (1966), *Psychological stress and the coping process*. New York: McGraw-Hill.

Lazarus, R. S. (1991), *Emotion and Adaptation*. Oxford, UK: Oxford University Press.

Lazarus, R.S., & Folkman, S. (1984), *Stress, appraisal, and coping*. New York: Springer Publishing Company.

Leclercq-Vandelannoitte, A. (2015a), Leaving employees to their own devices: new practices in the workplace. *Journal of Business Strategy*, vol. 36, n°5, p. 18-24.

Leclercq-Vandelannoitte, A. (2015b), Managing BYOD: how do organizations incorporate user-driven IT innovations? *Information Technology & People*, vol. 28, n°1, p. 2-33.

Lee, Y., & Larsen, K.R. (2009), Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, vol. 18, n°2, p. 177-187.

Lee, C., Lee, C.C., & Kim, S. (2016), Understanding information security stress: Focusing on the type of information security compliance activity. *Computers & Security*, vol. 59, p. 60-70.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019), Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, vol. 45, p. 13-24.

Li, H., Sarathy, R., & Xu, H. (2011), The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems*, vol. 51, n°3, p. 434-445.

Liang, H., Saraf N., Hu Q., & Xue Y. (2007), Assimilation of Enterprise Systems: the Effect of Institutional Pressures and the Mediating Role of top Management. *MIS Quarterly*, vol. 31, n°3, p. 59-87.

Liang, H., & Xue, Y. (2009), Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly*, vol. 33, n°1, p. 71-90.

Liang, H., & Xue Y. (2010), Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. *Journal of the Association for Information Systems*, vol. 11, n°3, p. 394-413.

Liang, H., Xue, Y., Pinsonneault, A., & Wu, Y. (2019), What Users Do Besides Problem-focused Coping When Facing IT Security Threats: An Emotion-Focused Coping Perspective. *MIS Quarterly*, vol. 43, n°2, p. 373-394.

Limayem, M., & Hirt, S. G. (2003), Force of Habit and Information Systems Usage: Theory and Initial Validation. *Journal of the Association for Information Systems*, vol. 4, n°1, p. 65-97.

Limayem, M., Hirt, S. G., & Cheung, C. M. K. (2007), How Habit Limits the Predictive Power of Intention: The Case of Information Systems Continuance. *MIS Quarterly*, vol. 31, n°3, p. 705-737.

Lin, T.-C., Ku, Y.-C., & Huang, Y.-S. (2014), Exploring Top Managers' Innovative IT (IIT) Championing Behavior: Integrating the Personal and Technical Contexts. *Information & Management*, vol. 51, n°3, p. 1-12.

Liu, G., Wang, E., & Chua, C. (2015), Leveraging Social Capital to Obtain Top Management Support in Complex, Cross-Functional IT Projects. *Journal of the Association for Information Systems*, vol. 16, n°3, p. 707-737.

Maddux, J.E., & Rogers, R.W. (1983), Protection Motivation and Self-efficacy: A Revised Theory of Fear Appeals and Attitude Change. *Journal of Experimental Social Psychology,* vol. 19, n°5, p. 469-479.

Malhotra, N.K., Kim, S.S., & Agarwal, J. (2004), Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, vol. 15, n°4, p. 336-355.

Martens, M., De Wolf, R. & De Mareza, L. (2019), Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. *Computers in Human Behavior*, vol. 92, p. 139-150.

McComb, S. A., Kennedy, D. M., Green, S. G., & Compton, W. D. (2008), Project Team Effectiveness: The Case for Sufficient Setup and Top Management Involvement. *Production Planning & Control*, vol. 19, n°3, p. 301-311.

McKeen, J.D., & Smith, H.A. (2007), Strategic Experimentation with IT. *Communications of the AIS*, vol. 19, p. 132-141.

McQuivey, J. (2013), How CIOs can be disruptors and exploit digital economies of scale. *ComputerWeekly*, 21 mai, p. 14-14.

Messeghem, K., & Torrès, O. (Dir) (2015), *Les grands auteurs en Entrepreneuriat et PME*. Editions EMS, Cormelles-le-Royal.

Meyer, J.W., & Rowan, B. (1977), Institutionalized organizations: formal structure as myth and ceremony. *American Journal of Sociology*, vol. 83, n°2, p. 340-363.

Miles, M. B., & Huberman, A.M. (2003), *Analyse des données qualitatives*, De Boeck, Bruxelles.

Mohd Salleh, N.A., Rohde, F., & Green, P. (2017), Information Systems Enacted Capabilities and Their Effects on SMEs' Information Systems Adoption Behavior. *Journal of Small Business Management*, vol. 55, n°3, p. 332-364.

Moody, G.D., Siponen, M., & Pahnila, S. (2018), Toward a Unified Model of Information Security Policy Compliance. *MIS Quarterly*, vol. 42, n°1, p. 285-311.

Moore, G. C., & Benbasat, I. (1991), Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information Systems Research*, vol. 2, n°3, p. 192-222.

Moorman, C., & Miner, A.S. (1998), Organizational improvisation and organizational memory. *Academy of Management Review*, vol. 23, p. 698-723.

Moser, S., Bruppacher, S.E., & Mosler, H.-J. (2011), How people perceive and will cope with risks from the diffusion of ubiquitous information and communication technologies. *Risk Analysis*, vol. 31, n°5, p. 832-846.

Motulsky, A., Wong, J., Cordeau, J.P., Pomalaza, J., Barkun, J., & Tamblyn, R. (2017), Using mobile devices for inpatient rounding and handoffs: an innovative application developed and rapidly adopted by clinicians in a pediatric hospital. *Journal of the American Medical Informatics Association*, vol. 24, n°e1, p. e69-e78.

Mueller, M., Klesel, M., Heger, O., & Niehaves, B. (2016), Empirical insights on individual innovation behavior: A qualitative study on IT-Consumerization. *Pacific Asia Conference on Information Systems (PACIS)*, Chiayi, Taiwan.

Mwagwabi, F., McGill, T., & Dixon, M. (2018), Short-Term and Long-Term Effects of Fear Appeals in Improving Compliance with Password Guidelines. *Communications of the Association for Information Systems,* vol. 42, n°3, p. 147–192.

Nance, W.D., & Straub, D.W. (1988), An Investigation into the Use and Usefulness of Security Software in Detecting Computer Abuse. *ICIS Proceedings*. 36. https://aisel.aisnet.org/icis1988/36.

Ng, B.-Y., Kankanhalli, A., & Xu, Y. (2009), Studying Users' Computer Security Behavior: A Health Belief Perspective. *Decision Support Systems*, vol. 46, n°3, p. 815-825.

Nobre, T. (2013), L'innovation managériale à l'hôpital. Changer les principes du management pour que rien ne change ? *Revue Française de Gestion*, vol. 6, n°235, p. 113-127.

Ortbach, K., Köffer, S., Bode, M., & Niehaves, B. (2013), Individualization of Information Systems-Analyzing Antecedents of IT Consumerization Behavior. *Thirty Fourth International Conference on Information Systems (ICIS)*, Milan, Italy.

Ozgen, E., & Baron, R. A. (2007), Social Sources of Information in Opportunity Recognition: Effects of Mentors, Industry Networks, and Professional Forums. *Journal of Business Venturing*, vol. 22, n°3, p. 174-192.

Palfrey, J. G., & Gasser, U. (2013), *Born digital: Understanding the first generation of digital natives*. Basic Books.

Palich, L.E., & Bagby, D.R. (1995), Using cognitive theory to explain entrepreneurial risk-taking: challenging conventional wisdom. *Journal of Business Venturing*, vol. 10, n° 6, p. 425-438.

Park, H.-J., & Cho, J.-S. (2016), The influence of information security technostress on the job satisfaction of employees. *Journal of Business and Retail Management Research*, vol. 11 n°1, p. 66-75.

Polites, G. L., & Karahanna, E. (2013), The embeddedness of Information Systems Habits in Organizational and Individual-Level Routines: Development and Disruption. *MIS Quarterly*, vol. 37, n°1, p. 221-246.

Posey, C., Roberts, T. L., & Lowry, P. B. (2015), The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets. *Journal of Management Information Systems*, vol. 32, n°3, p. 179-214.

Pras, B. (2012), Entreprise et vie privée : le 'privacy paradox' et comment le dépasser ? *Revue Française de Gestion*, vol. 5, n°224, p. 87-94.

Pritchard, S. (2010), Navigating the black hole of small business security. *Infosecurity*, Sept.-Oct., p. 18-21.

Ragu-Nathan, B. S., Apigian, C. H., Ragu-Nathan, T. S., & Tu, Q. (2004), A Path Analytic Study of the Effect of Top Management Support for Information Systems Performance. *Omega*, vol. 32, n°3, p. 459-471.

Ragu-Nathan, T.S., Tarafdar, M., Ragu-Nathan, B.S., & Tu, Q. (2008), The Consequences of Technostress for End Users, in Organizations: Conceptual Development, and Empirical Validation. *Information Systems Research*, vol. 19, n°4, p. 417-433.

Roberts, N., & Grover, V. (2012), Leveraging IT Infrastructure to Facilitate a Firm's Customer Agility and Competitive Activity: An Empirical Investigation. *Journal of Management Information Systems*, vol. 28, n°4, p. 231-269.

Rogers, R.W. (1983), Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo & R. E. Petty (Eds.), *Social psychophysiology: A sourcebook* (p. 153-176). New York: Guilford Press.

Ryan, J.J.C.H. (2004), Information Security Tools and Practices: What Works? *IEEE Transactions on Computers,* vol. 53, n°8, p. 1060-1063.

Safa, N.S., von Solms, R., Furnell, S. (2016), Information security policy compliance model in organizations. *Computers & Security*, vol. 56, p. 70-82.

Sarstedt, M., Ringle, C. M., Smith, D., Reams, R., & Hair, J. F. (2014), Partial Least Squares Structural Equation Modeling (PLS-SEM): A Useful Tool for Family Business Researchers. *Journal of Family Business Strategy*, vol. 5, n°3, p. 105-115.

Schmitt, C. (2015), *L'agir entrepreneurial : Repenser l'action des entrepreneurs*. Presses de l'Université du Québec, Québec.

Schoonjans, B., van Cauwenberge, P., & Bauwhede, H. V. (2013), Formal Business Networking and SME Growth. *Small Business Economics*, vol. 41, n°3, p. 169-181.

Sheng, H., Nah, F. F.-H., & Siau, K. (2008), An Experimental Study on Ubiquitous Commerce Adoption: Impact of Personalization and Privacy concerns. *Journal of the AIS*, vol. 9, n°6, p. 344-376.

Singh, N. (2012), B.Y.O.D. Genie Is Out of the Bottle – 'Devil or Angel'. *Journal of Business Management & Social Sciences Research*, vol. 1, n°3, p. 1-12.

Siponen, M., Mahmood, M.A., & Pahnila, S. (2014), Employees' adherence to information security policies: An exploratory field study. *Information & Management*, vol. 51, n°2, p. 217-224.

Sivarajah, U., Kamal, M.M., Irani, Z., & Weerakkody, V. (2017), Critical analysis of Big Data challenges and analytical methods. *Journal of Business Research*, vol. 70, p. 263-286.

Sommestad, T., Karlzén, H., & Hallberg, J. (2015), The Sufficiency of the Theory of Planned Behavior for Explaining Information Security Policy Compliance. *Information and Computer Security*, vol. 23, n°2, p. 200-217.

Spears, J.L., Barki, H., Barton, R.R. (2013), Theorizing the concept and role of assurance in information systems security. *Information & Management*, vol. 50, n° 7, p. 598-605.

Srivastava, S.C., Chandra, S., & Shirish, A. (2015), Technostress creators and job outcomes: theorising the moderating influence of personality traits. *Information Systems Journal*, vol. 25, p. 355-401.

Straub, D.W., & Welke, R. (1998), Coping with systems risk: security planning models for management decision making. *MIS Quarterly*, vol. 22, n°4, p. 441-469.

Sultan, N. (2013), Cloud computing: A democratizing force? *International Journal of Information Management,* vol. 33, p. 810-815.

Sutanto, J., Palme, E., Tan, C.-H., & Phang, C.W. (2013), Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users. *MIS Quarterly*, vol. 37, n° 4, p. 1141-1164.

Tallon, P.P., & Pinsonneault, A. (2011), Competing Perspectives on the Link between Strategic Information Technology Alignment and Organizational Agility: Insights from a Mediation Model. *MIS Quarterly*, vol. 35, n°2, p. 463-486.

Tarafdar, M., Tu, Q., Ragu-Nathan, B. S., & Ragu-Nathan, T. S. (2007), The impact of technostress on role stress and productivity. *Journal of Management Information Systems*, vol. 24, n°1, p. 301-328.

Taylor, S., & Todd, P.A. (1995), Understanding Information Technology Usage: A Test of Competing Models. *Information Systems Research*, vol. 6, n°4, p. 144-176.

Templier, M., & Paré, G. (2017), Transparency in literature reviews: an assessment of reporting practices across review types and genres in top IS journals. *European Journal of Information Systems*, p. 1-48, https://doi.org/10.1080/0960085X.2017.1398880.

Thompson, R. L., Higgins, C. A., & Howell, J. M. (1991), Personal Computing: Toward a Conceptual Model of Utilization. *MIS Quarterly*, vol. 15, n°1, p. 124-143.

Thompson, N., McGill, T. J., & Wang, X. (2017), "Security Begins at Home": Determinants of Home Computer and Mobile Device Security Behavior. *Computers & Security,* vol. 70, n°3, p. 376-391.

Tobler, N., Colvin, J., & Rawlins, N.W. (2017), Longitudinal Analysis and Coping Model of User Adaptation. *Journal of Computer Information Systems*, vol. 57, n°2, p. 97-105.

Torten, R., Reaiche, C., & Boyle, S. (2018), The impact of security awarness on information technology professionals' behavior. *Computers & Security*, vol. 79, p. 68-79.

Tsai, H.-Y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotton, S. R. (2016), Understanding Online Safety Behaviors: A Protection Motivation Theory Perspective. *Computers & Security*, vol. 59, n°3, p. 138-150.

Tu, Z., Turel, O., Yuan, Y., & Archer, N. (2015), Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination. *Information & Management*, vol. 52, n°4, p. 506-517.

Urwiler, R., & Frolick, M. N. (2008), The IT Value Hierarchy: Using Maslow's Hierarchy of Needs as a Metaphor for Gauging the Maturity Level of Information Technology Use within Competitive Organizations. *Information Systems Management*, n°25, p. 83-88.

Vallerand, R. J. (1997), Toward a Hierarchical Model of Intrinsic and Extrinsic Motivation, in *Advances in Experimental Social Psychology*, vol. 29, M. Zanna (ed.), Academic Press, New York, p. 271-360.

Van Gelderen, M., Kautonen, T., & Fink, M. (2015), From entrepreneurial intentions to actions: Self-control and action-related doubt, fear, and aversion. *Journal of Business Venturing*, vol. 30, p. 655–673.

Van Riel, A.C.R., Henseler, J., Kemeny, I., & Sasovova, Z. (2017), Estimating hierarchical constructs using consistent partial least squares: The case of second-order composites of common factors. *Industrial Management & Data Systems*, vol. 117, n°3, p. 459-477.

Vance, A., Siponen, M., & Pahnila, S. (2012), Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, vol. 49, n°3-4, p. 190-198.

Varela, F.V., Thompson, E., & Rosch, E. (1992), *The embodied mind: Cognitive science and human experience*. MIT Press. p. 9.

Venkatesh, V., Brown, S.A., & Bala, H. (2013), Bridging the Qualitative-Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems. *MIS Quarterly*, vol. 37, n°1, p. 21-54.

Venkatesh, V., & Davis, F. D. (2000), A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Management Science*, vol. 45, n°2, p. 186-204.

Venkatesh, V., Morris, M.G., Davis, G.B., & Davis, F.D. (2003), User acceptance of information technology: Toward a unified view. *MIS Quarterly*, vol. 27, n°3, p. 425-478.

Venkatesh, V., & Speier, C. (1999), Computer Technology Training in the Workplace: A Longitudinal Investigation of the Effect of the Mood. *Organizational Behavior and Human Decision Processes*, vol. 79, n°1, p. 1-28.

Venkatraman, N. (1991), IT-Induced Business Reconfiguration: The New Strategic Management Challenge, in Scott Morton ed., *The Corporation of the 1990s*, New York: Oxford University Press.

Venters, W., & Whitley, E.A. (2012), A critical review of cloud computing: researching desires and realities. *Journal of Information Technology*, n° 27, p. 179-197.

Wang, X., Weeger, A., Gewald, H., Sanchez, O., Raisinghani, M., & Pittayachawan, S. (2015), Determinants of intention to participate in corporate BYOD-programs: The case of digital natives. *75th Annual Meeting of the Academy of Management*, 7-11 August, Vancouver, BC Canada.

Warkentin, M., Johnston, A.C., Shropshire, J., & Barnett, W. D. (2016), Continuance of Protective Security Behavior: A Longitudinal Study. *Decision Support Systems*, vol. 92, n°3, p. 25-35.

Weeger, A., Wang, X., & Gewald, H. (2016), IT consumerization: BYOD-program acceptance and its impact on employer attractiveness. *Journal of Computer Information Systems*, vol. 56, n°1, p. 1-10.

Weick, K.E. (1993), The collapse of sensemaking in organizations: the Mann gulch disaster. *Administrative Science Quarterly*, vol. 38, p. 628-652.

Whitten, D., Hightower, R., & Sayeed, L. (2014), Mobile device adaptation efforts: The impact of hedonic and utilitarian value. *Journal of Computer Information Systems*, vol. 55, n°1, p. 48-58.

Williams, C. K., Wynn, D., Madupalli, R., Karahanna, E., & Duncan, B. K. (2014), Explaining Users' Security Behaviors with the Security Belief Model. *Journal of Organizational and End User Computing*, vol. 26, n°3, p. 23-46.

Witte, K. (1992), Putting the Fear Back into Fear Appeals: The Extended Parallel Process Model. *Communication Monographs*, vol. 59, n°4, p. 329-349.

Workman, M., Bommer, W.H., & Straub, D. (2008), Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test. *Computers in Human Behavior,* vol. 24, n°6, p. 2799-2816.

Workman, M., & Gathegi, J. (2005), Observance and contravention of information security measures. *In Proceedings of the world conference on security management and applied computing*, p. 241-247, Las Vegas, NV.

Xue, L., Zhang, C., Ling, H., & Zhao X. (2013), Risk Mitigation in Supply Chain Digitization: System Modularity and Information Technology Governance. *Journal of Management Information Systems*, vol. 30, n°1, p. 325-352.

Yazdanmehr, A., & Wang, J. (2016), Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems*, vol. 92, p. 36-46.

Yun, H., Kettinger, W. J., & Lee, C. C. (2012), A New Open Door: The Smartphone's Impact on Work-to-Life Conflict, Stress, and Resistance. *International Journal of Electronic Commerce*, vol. 16, n°4, p. 121-151.

# Table des Matières

# Curriculum Vitae détaillé

Yves BARLETTE
Né le 3 février 1964 à Carcassonne (Aude)
Deux enfants.

Professeur en Systèmes d'Information
Montpellier Business School
2300, Avenue des Moulins
34185 Montpellier Cedex 4.

## Publications

*Thèse de Doctorat*

*Les comportements sécuritaires des acteurs dans les systèmes d'information des PME.*
Université de Montpellier, soutenue le 15 décembre 2006.

*Articles parus ou acceptés dans des revues à comité de lecture (CNRS 06/2020 – FNEGE 2019)*

| Réf. | Articles | Classement CNRS/FNEGE |
|---|---|---|
| PPC, 2020 | Barlette Y. & Baillette P. 2020. Big Data Analytics in turbulent contexts: Towards organizational change for enhanced agility. *Production Planning & Control*, 32, DOI: 10.1080/09537287.2020.1810755. | 2/2 Internationale |
| JGIM, 2020 | Baillette P. & Barlette Y. 2020. Coping Strategies and Paradoxes Related to BYOD Information Security Threats in France, *Journal of Global Information Management*, 28(2): 1-28.<br>(*) La revue a été déclassée en rang 3 dans la classification CNRS 11/2018 publiée en 02/2019. | 2(*)/3 Internationale |
| SIM, 2019 | Barlette Y. & Jaouen A. 2019. Information Security in SMEs: Determinants of CEOs' Protective and supportive Behaviors. *Systèmes d'Information et Management*, 24(3): 7-40. | 2/2 |
| IJIM, 2018 | Baillette P., Barlette Y. & Leclercq-Vandelannoitte A. 2018. Bring Your Own Device in organizations: Extending the reversed IT adoption logic to security paradoxes for CEOs and end-users, *International Journal of Information Management*, 43(December): 76-84.<br>(**) La revue a été reclassée en rang 2 dans la classification FNEGE publiée en juin 2019. | 3/3(**) Internationale |
| P&MP, 2018 | Baillette P. & Barlette Y. 2018. BYOD et innovations managériales en contexte hospitalier : mise en évidence d'une logique d'adoption inversée, *Politiques et Management Public*, 35(1): 49-68. | 4/4 |
| JOCM, 2018 | Baillette P. & Barlette Y. 2018. BYOD-related innovations and organizational change for entrepreneurs and their employees in SMEs: the identification of a twofold security paradox, *Journal of Organizational Change Management*, 31(4): 839-851. | 3/3 Internationale |
| SIM, 2017 | Barlette Y., Gundolf K. & Jaouen A. 2017. CEOs' Information Security Behavior in SMEs: Does Ownership Matter? *Systèmes d'Information et Management*, 22(3): 7-45. | 2/2 |
| JIEM, 2016 | Maric J., Rodhain F. & Barlette Y. 2016. Frugal innovations and 3D printing: Insights from the field, *Journal of Innovation Economics & Management*, 2016/3(21): 57-76. | 4/4 |

| | | |
|---|---|---|
| MTO, 2016 | Maric J., Rodhain F. & Barlette Y. 2016. 3D printing trends and discussing societal, environmental and ethical implications, *Management des Technologies Organisationnelles*, 6: 126-138. | -/- |
| JISIB, 2015 | Barlette Y., Gundolf K. & Jaouen A. 2015. Toward a better understanding of SMB CEOs' Information Security Behavior: Insights from Threat or Coping appraisal, *Journal of Intelligence Studies in Business*, 5(1): 5-17. | -/- (classée NSD[24]) |
| MTO, 2015 | Barlette Y. 2015. Cloud Computing et Stratégie S.I., *Management des Technologies Organisationnelles*, 5: 62-74. | -/- |
| MTO, 2015b | Maric J., Rodhain F. & Barlette Y. 2015. Responsible innovation and reverse logistics, *Management des Technologies Organisationnelles*, 5: 212-220. | -/- |
| MTO, 2013 | Barlette Y. 2013. Les dangers des réseaux sociaux : comment s'en prémunir ?, *Management des Technologies Organisationnelles*, 3: 196-205. | -/- |
| SIM, 2012 | Barlette Y. 2012. Implication et action des dirigeants : quelles pistes pour améliorer la sécurité de l'information en PME, *Systèmes d'Information et Management*, 17(2): 115-149. | 2/2 |
| MTO, 2012 | Barlette Y. 2012. Vers une implication et une action des dirigeants de PME dans la sécurité de leur S.I., *Management des Technologies Organisationnelles*, 2: 277-306. | -/- |
| SIM, 2008 | Barlette Y. 2008. Une étude des comportements liés à la sécurité des systèmes d'information en PME. *Systèmes d'Information et Management,* 13(4): 7-30. | 2/2 |
| R2I, 2004 | Barlette Y. 2004. Le facteur humain dans l'amélioration de la sécurité des informations : l'importance des directions d'entreprises. *Revue Internationale en Intelligence Informationnelle*, 1. | -/- |
| CG, 2002 | Barlette Y. 2002. Les intrusions sur le Web : Vers un modèle de risque perçu par les entreprises, *Revue Cyber-Gestion*, 6. | -/- |

*Articles en cours de révision ou sur le point d'être soumis (CNRS 06/2020 – FNEGE 2019)*

| Tour et date soumission | **Articles** | Classement CNRS/FNEGE |
|---|---|---|
| IJIM, R3 Aug. 2020 | Barlette Y., Jaouen A. & Baillette P. Bring Your Own Device (BYOD) as a reversed IT adoption: Insights into Managers' Coping Strategies. *International Journal of Information Management.* | 3/2 Internationale |
| IJIM, R1 Nov. 2020 | Baillette P. & Barlette Y. Security and confidentiality in health information: new risks stemming from mobile device implementation and how to mitigate them, *International Journal of Information Management.* | 3/2 Internationale |
| EJIS, R1 Dec. 2020 | Barlette Y. & Berthevas J.-F. Examining employees' coping behavior related to Shadow IT adoption. *European Journal of Information Systems*. | 1/1 Internationale |

[24] Norwegian Register for Scientific Journals

*Ouvrages*

Barlette Y., Bonnet D., Plantié M. & Riccio P.-M. 2017. *Numérique et Organisations*, Paris, Presses des Mines.

Barlette Y., Bonnet D., Plantié M. & Riccio P.-M. 2016. *Désordres numériques : incertitude et opportunités*, Paris, Presses des Mines.

Barlette Y., Bonnet D., Plantié M. & Riccio P.-M. 2015. *Réseaux numériques et performance des entreprises*, Paris, Presses des Mines.

Barlette Y., Bonnet D., Plantié M. & Riccio P.-M. 2014. *De l'innovation technologique à l'innovation managériale*, Paris, Presses des Mines.

Barlette Y., Bonnet D., Plantié M. & Riccio P.-M. 2013. *Impact des réseaux numériques dans les organisations,* Paris, Presses des Mines.

*Chapitres d'ouvrages*

Barlette Y. & Jaouen A. 2014. La relation entre le dirigeant et son expert-comptable en matière de gestion des informations. In Lecointre G. (Ed.), *Le Grand Livre de l'Economie PME 2015 : 629-648*, Paris, Gualino.

Barlette Y. 2014. Les Systèmes d'Information. In Marques P. & Granata J. (Eds.), *DUT GEA 2ème année* : 353-375, Paris, Dunod.

Maric J., Rodhain F. & Barlette Y. 2014. Information Systems and Reverse Logistics: Examining Drivers of Implementation on Multiple Case-Study Scenario, In W. Kersten, T. Blecker & C.M. Ringle (Eds.). *Next Generation Supply Chains: 211-221*, Berlin, epubli GmbH.

Barlette Y., Den Besten, M. & Khédiaoura A. 2013. Les innovations et le Management des Systèmes d'Information. In A. Jaouen & F. Le Roy (Eds.). *Innovation managériale* : 181-202, Paris, Dunod.

Barlette Y. 2011. Gérer ses informations et les protéger in K. Gundolf et A. Jaouen (Eds.), *Diriger sa petite entreprise. Gérer, communiquer, se développer : 45-60*, Paris, Dunod.

Barlette Y. & Fomin V.V. 2010. The Adoption of Information Security Management Standards: A Literature Review in Information Resources Management Association (Eds.). *Information Resources Management: Concepts, Methodologies, Tools and Applications:* 69-90, IGI Global, USA.

Barlette Y. & Fomin, V.V. 2009. The adoption of Information Security management Standards: A Literature Review. In Knapp K.J. (Ed.), *Cyber-Security & Global Information Assurance: Threat, analysis and response solutions: 119-140,* IGI Global, USA.

Barlette Y. 2005. L'apport des facteurs éthiques à la sécurité des informations : une revue de la littérature. In S. Agostinelli, *L'éthique des situations de communication numérique* : 145-163. Paris, L'Harmattan.

## Communications

Barlette Y. & Berthevas J.-F. 2020. Examining Employees' coping behavior related to Shadow IT adoption. *25ème congrès international de l'AIM,* Conférence en ligne, 11-12 Juin.

Baillette P., Barlette Y. & Jaouen A. 2019. Evaluation et choix entre modèles avec SmartPLS : application au CMUA et à la PMT, *24ème congrès international de l'AIM,* June 4-5, Nantes, France.

Baillette P., Barlette Y. 2019. Innovations managériales à l'hôpital et risques relatifs au BYOD dans le contexte du RGPD, *Workshop TI et santé*, 24 May, Montpellier, France.

Maric J., Barlette Y. & Rodhain F. 2018. 3D printing technology adoption in the context of the collaborative working spaces, *AIMS XXVII*, June 6-8, Montpellier, France.

Maric J., Barlette Y. & Rodhain F. 2018. Adoption and tendencies of 3D printing technology in the context of the Makers culture, *3rd Innovation days*, April 3-4, Paris, France.

Baillette P. & Barlette Y. 2018. Examining CEOs' Behavior related to BYOD implementation through the CMUA, *23ème congrès international de l'AIM,* May 16-18, Montréal, Canada.

Maric J., Barlette Y. & Rodhain F. 2018. The importance of co-working spaces in 3D printing technology adoption and diffusion, *23ème congrès international de l'AIM,* May 16-18, Montréal, Canada.

Baillette P. & Barlette Y. 2017. Outils mobiles et innovations en milieu hospitalier : qu'en est-il de leur management ?, *Journée de recherche thématique UPVD* "Innovation, numérique et entreprise: quels enjeux pour le management de demain ?", June 8, Perpignan, France.

Baillette P. & Barlette Y. 2017. Security paradox situations related to the BYOD phenomenon in SMEs: Insights from the Coping Model of User Adaptation, *22ème congrès international de l'AIM*, May 17-19, Paris, France.

Baillette P. & Barlette Y. 2016. Identification of the 'security paradox' in SMEs: application to BYOD-related practices, *Pre-ICIS Workshop on Information Security and Privacy (WISP)*, December 10, Dublin, Ireland.

Barlette Y. 2016. Agilité organisationnelle et alignement stratégique : revue de la littérature et pistes de recherche, *21ème congrès international de l'AIM*, May 18-20, Lille, France.

Maric J., Rodhain F. & Barlette Y. 2016. Disruptiveness in the context of 3D printing technology, *21ème congrès international de l'AIM*, May 18-20, Lille, France.

Maric J., Rodhain F. & Barlette Y. 2016. Practical acceptability of responsible innovation, *Forum Innovation VII*, June 9-11, Paris, France.

Maric J., Rodhain F. & Barlette Y. 2016. Discussions on Disruptive Potential of the 3D Printing Technology, *Information and Communication Technologies in Organizations and Society (ICTO)*, March 3-4, Paris, France.

Maric J., Rodhain F. & Barlette Y. 2015. Is 3D printing next big thing?, 7ème *colloque MTO*, October 8-9, Montpellier, France.

Barlette, Y. 2015. Big Data et outils analytiques : incertitude et opportunités, 7ème *colloque MTO*, October 8-9, Montpellier, France.

Maric J., Rodhain F. & Barlette Y. 2015. Open and Responsible Innovations for Creating Competitive Advantage, *9th Mediterranean Conference on Information Systems (MCIS)* - I.S. in a Changing Economy and Society, October 3-5, Samos, Greece.

Maric J., Rodhain F. & Barlette Y. 2015. Information Systems and Reverse Logistics: Promise for Future, *International Conference on Circuits and Systems (CAS 2015),* August 9-10, Paris, France.

Maric J., Rodhain F. & Barlette Y. 2015. Discussions on practical acceptability of responsible innovation concept in management innovation, *EURAM*, July 9-10, Montpellier, France.

Barlette Y., Gundolf K. & Jaouen A. 2015. Toward a better understanding of SMB CEOs' Information Security Behavior: Insights from Threat or Coping appraisal, *20ème congrès international de l'AIM*, May 20-22, Rabat, Morocco.

Maric J., Rodhain F. & Barlette Y. 2015. Examining responsible innovation concept of integrated reverse logistic model, *20ème congrès international de l'AIM*, May 20-22, Rabat, Morocco.

Maric J., Rodhain F. & Barlette Y. 2014. Examining drivers of reverse logistics implementation as responsible innovation, 6ème *colloque MTO*, October 2-3, Nîmes, France.

Maric J., Rodhain F. & Barlette Y. 2014. Information Systems and Reverse Logistics: Concept and Management Paradigm Shift, *Hamburg International Conference of Logistics (HICL)*, September 18-19, Hamburg, Germany.

Maric J., Rodhain F. & Barlette Y. 2014. Information Systems and Reverse Logistics: Promise for Future? 3rd *International Conference on Challenges in Environmental Science and Computer Engineering* (CESCE), June 21-22, London, England.

Barlette Y. 2014. Vers une meilleure exploitation des Technologies Numériques, *6ème Colloque Management des Technologies Organisationnelles (MTO)*, October 2-3, Nîmes, France.

Barlette Y. 2014. L'évolution du rôle du DSI : Etat de l'art et identification de pistes de recherche, *19ème congrès international de l'AIM*, May 20-21, Aix-Marseille, France.

Barlette Y. & Jaouen A. 2012. What is the influence of certified public accountants on microfirm owner-managers*? XXVIth Research in Entrepreneurship and Small Business Conference (RENT)*, November 21-23, Lyon, France.

Barlette Y. & Jaouen A. 2012. Quelle est l'influence de l'expert-comptable sur le dirigeant de TPE ? Le cas de la gestion des informations de l'entreprise*. 11ème congrès international CIFEPME*, October 24-26, Brest, France.

Barlette Y. 2012. Les dangers des réseaux sociaux : comment s'en prémunir ? *4ème colloque Management des Technologies Organisationnelles (MTO)*, October 4-5, Nîmes, France.

Barlette Y. & Jaouen A. 2011. Influence de l'expert-comptable sur la prise de décision en matière de S.I. des dirigeants de TPE*. 16ème congrès international de l'AIM*, May 25-27, La Réunion, France.

Barlette Y. 2011. Implication, action des dirigeants de PME et niveau de sécurité de leur S.I. *16ème congrès international de l'AIM*, May 25-27, La Réunion, France.

Barlette Y. 2011. Vers une implication et une action des dirigeants de PME dans la sécurité de leur Système d'Information. *3ème colloque Management des Technologies Organisationnelles (MTO).* March 17-18, Nîmes, France.

Barlette Y. 2009. Vers une implication et une action des dirigeants de PME dans la sécurité de leur S.I. *14ème congrès international de l'AIM*, June 10-12, Marrakech, Morocco.

Barlette Y. 2008. L'adoption et la mise en place des normes relatives à la sécurité des S.I. : une revue de littérature. *13ème congrès International de l'AIM,* December 13-14, Paris, France.

Fomin V.V., DeVries H. J., and Barlette Y. 2008. ISO/IEC 27001 Information Systems Security Management Standard: Identifying Directions for Future Research. *3rd European Conference on Management of Technology (EuroMOT)*, September 17-19, Nice Sophia Antipolis, France.

Barlette Y. & Fomin V.V. 2008. Exploring the suitability of IS security management standards for SMEs. *41st annual Hawaii International Conference on System Sciences (HICSS),* January 7-10, Computer Society Press, Big Island, Hawaii, USA.

Barlette Y. 2007. Les acteurs des PME face à la protection des S.I. *5èmes rencontres en intelligence Economique*, September 7, Nice Sophia Antipolis, France.

Barlette Y. 2007. Les comportements sécuritaires des acteurs dans les systèmes d'information des PME. *12ème congrès international de l'AIM*, June 18-19, Lausanne, Switzerland.

Barlette Y. 2007. La sécurité des informations n'est pas réservée aux grandes entreprises. *18ème conférence EUROSEC,* 23-25 mai, Paris, France.

Barlette Y. 2006. Les comportements sécuritaires des acteurs en PME. 3ème *Colloque Intelligence Informationnelle*, June 29-30, Paris, France.

Barlette Y. 2005. L'implication des décideurs détermine les comportements sécuritaires des acteurs en PME. *10ème congrès international de l'AIM*, September 22-23, Toulouse, France.

Barlette Y. 2004. La sécurité des informations : de la perception des risques à un modèle holistique. 2nd *colloque Intelligence informationnelle*, Plaine St Denis, 1-2 Juin, Paris, France.

Barlette Y. 2003. Sécurisation des processus et processus de sécurisation dans les Dot Com. *Management des Entreprises électroniques,* December 12, Montpellier, France.

Barlette Y. 2003. Comment créer et conserver la confiance du consommateur dans le commerce électronique. *1er colloque Intelligence Informationnelle,* May 20, Paris, France.

## Organisation de colloques

2020: Pré-ICIS AIM Workshop "digitalisation et risques", December 12, Online. (Organization team member).

2016: *8th Conference Management des Technologies Organisationnelles (MTO),* October 6-7, Nîmes, France. (Organization team member).

2015: EURAM Thematic Conference 2015 'Management Innovation: new borders for a new concept', July 9-10, Montpellier, France. (Organization team member).

2015: *7th Conference Management des Technologies Organisationnelles 2015 (MTO),* October 8-9, Montpellier, France. (Organization team member, chair of tracks 3 & 6).

2014: *6th Conference Management des Technologies Organisationnelles 2014 (MTO),* October 2-3, Nîmes, France. (Organization team member).

2013: *5th Conference Management des Technologies Organisationnelles 2013 (MTO),* October 3-4, Montpellier, France. (Organization team member).

2012: *4th Conference Management des Technologies Organisationnelles 2012 (MTO),* October 4-5, Nîmes, France. (Organization team member).

2011: *3rd Conference Management des Technologies Organisationnelles 2011 (MTO),* March 17-18, Nîmes, France. (Organization team member).

2007: *Montpellier International Workshop on Information Systems and Organization Dynamics,* July 13, Montpellier, France. (Organization team member).

2003: *Colloque Montp'2003 - manager l'entreprise électronique,* December 12, Montpellier, France. (Organization team member).

2001: *Workshop on information security,* May 30-31, University of Montpellier I, France. (Organization team member).

## Projets

2008 : Projet ITEA-2. Cet appel à projet avait pour vocation de stimuler et soutenir des projets de R&D innovants et pré-concurrentiels afin de contribuer à l'excellence de la recherche Européenne en systèmes et services à forte intensité logicielle. Les principaux acteurs que j'ai côtoyés sont : Mikko Siponen du Department of Information Processing Science, the University of Oulu Christer Magnusson du Department of Computer and Systems Sciences, Stockholm University Maria Karyda du Department of Information and Communication Systems Engineering, University of the Aegean, Greece.

2016 : Projet 'entreprendre' « Innovation, Entrepreneurship & CSR – An ICT and Gender Perspective ». Ce projet mêlait des acteurs locaux comme Isabelle bourdon et Anne-Laurence Laffont à des personnes externes : Guénola Nonet, Sophia Belghiti-Mahut, Guy Paré, Claudio Vitari, Chris Kimble, Sanaa Ait-Daoud.

Seules les phases de constitution de ces deux projets ont été réalisées, car ils n'ont pas été acceptés et ne se sont donc pas concrétisés. Mais, grâce à ces initiatives, j'ai pu développer des relations notamment avec Mikko Siponen et Guy Paré.

## Autres activités de recherche

*Prix et distinctions*

2018: 'Outstanding Contributor in Reviewing' certificate for the International Journal of Information Management, July.

2017: AIM-CIGREF Best reviewer award AIM 2017, May 18th, Paris, France.

2015: AIM-CIEMS Best paper award AIM 2015 for "Toward a better understanding of SMB CEOs' Information Security Behavior: Insights from Threat or Coping appraisal".

*Révision d'articles pour des revues*

| Période | Rang | Nom de la revue | Révisions |
|---|---|---|---|
| 2018-2020 | 3→2 | International Journal of Information Management | 15 |
| 2017-2019 | 3 | Journal of Organizational Change Management | 2 |
| 2010-2020 | 2 | Systèmes d'Information et Management | 10 |
| 2014-2016 | - | Management des Technologies Organisationnelles | 19 |
| 2015-2015 | 3 | Revue d'Economie Industrielle | 1 |
| *2014-2014* | 4 | Innovations - Journal of Innovation Economics & Management | 1 |
| 2009-2012 | 2 | Information & Management | 19 |

*Prise de responsabilité dans des revues*

10/2019- : Membre de l'International Editorial Review Board (IERB) de la revue *International Journal of Information Management* (Rang 2).

06/2013-06/2016 : Coéditeur en chef de la revue *Management des Technologies Organisationnelles*.

06/2009-06/2012 : Membre de l'Editorial Board de la revue *Information & Management* (Rang 2).

*Révision d'articles et responsabilités lors de conférences*

Association Information et Management (AIM)

- Deux à quatre révisions par an depuis 2007 ;
- Track chair en 2014, 2017 et 2020 ;
- Consortium doctoral en 2015 et 2019.

ICIS (2008) et ECIS (2016) : une révision, HICSS (2020) : deux révisions.

*Responsabilité de Groupe Thématique*

Depuis Septembre 2019 : Responsable du groupe thématique "sécurité de l'information" de l'AIM (GT AIM-SSI).

*Contributeur pour le Journal Quality List (JQL)*

Depuis 2015, j'informe Anne-Wil Harzing des systèmes de classement français et changements dans ces classements (FNEGE, CNRS, HCERES). Elle m'a inclus en 'special thanks' (p. 2 de chaque édition depuis 2015).

*Participation à des comités de thèse*

Participation régulière entre 2013 et 2018.

*Présentations devant l'équipe de recherche MRM-SI*

2019-2020 : 2 présentations.
2018-2019 : 3 présentations.
2015-2016 : 2 présentations.
2014-2015 : 1 présentation.
2013-2014 : 1 présentation.
2012-2013 : 2 présentations.

## Encadrements de thèses et mémoires

*Co-encadrement de doctorants*

09/2013 - 11/2018 : Josip Maric. Co-encadrement avec Florence Rodhain / Université de Montpellier - MRM. "*Sustainability and Responsibility in the Digitalization Era – A Study of Consumer-Level 3D Printing Technology*". Thèse soutenue le 2 novembre 2018.

10/2013 - 01/2015 : Myriam Criquet. Co-encadrement avec Nathalie Mallet-Poujol / ERCIM, équipe CNRS, UMR 5885 Dynamique du droit. « *Problématiques juridiques du Big Data* ». Thèse abandonnée.

*Thèses professionnelles de MBA (exercice académique)*

2018-2019 : Encadrement d'une thèse professionnelle de MBA.

2008-2009 : Encadrement d'une thèse professionnelle de MBA.

*Mémoires de Master 2 MBS (exercice académique)*

2020 : encadrement de 4 mémoires de master.

2019 : encadrement de 10 mémoires de master.

2018 : encadrement de 10 mémoires de master.

2017 : encadrement de 13 mémoires de master.

2016 : encadrement de 3 mémoires de master.

2015 : encadrement de 16 mémoires de master.

*Mémoires de Master 2 IAE (exercice académique)*

2017 : co-encadrement de 5 mémoires MTID.

2016 : co-encadrement de 10 mémoires MTID.

2008-2015 : encadrement et co-encadrement de 27 mémoires MTID.

*Mémoires de stage Master 2*

1996-2010 : encadrement de 225 mémoires de spécialisation « ingénieurs d'affaires en produits et services informatiques ».

2007-2007 : co-encadrement de 15 mémoires de l'école d'ingénieurs ESIEA.

2002-2007 : encadrement de 87 mémoires de spécialisation « e-business ».

## Cours enseignés ces 5 dernières années

| | | |
|---|---|---|
| **2013-2021:** Introduction to Information Systems (30h), | BL3, | MBS. |
| **2007-2021:** Advanced Information Systems (18h), | M2, | MBS & IAE Montpellier. |
| **2004-2021:** Sécurité de l'information (18h⇨ 9h 2018-), | M2, | MBS & IAE Montpellier. |
| **2019-2021:** Cybersecurity (15h), | MSc, | MBS. |
| **2012-2018:** Strategic Information Management (18h), | M2, | MBS & IAE Montpellier. |

# Liste des Annexes

# *Annexe 1 : Définition des principaux construits*

L'**attitude** comportementale est « *le ressenti positif ou négatif d'un individu (influence évaluative) concernant l'exercice d'un comportement précis* » (Fishbein et Ajzen, 1975, p. 216).

Les **normes subjectives** (ou influence sociale) correspondent à « *la perception par une personne, que la plupart des gens qui revêtent une importance pour elle, pense qu'elle devrait ou non accomplir le comportement en question* » (Fishbein et Ajzen, 1975, p. 302).

La **maîtrise perçue** du comportement (Ajzen, 1991) caractérise, une fois adaptée au champ des S.I. « *les perceptions des contraintes internes et externes portant sur le comportement* » (Taylor et Todd, 1995, p. 149).

**L'utilité perçue** ou performance espérée est « *le niveau de croyance d'une personne que le fait d'utiliser un système particulier pourra améliorer la performance dans son travail* » (Davis, 1989, p. 320).

La **facilité d'utilisation** perçue ou effort attendu correspond au « *niveau de croyance d'une personne que le fait d'utiliser un système particulier pourrait ne pas nécessiter d'effort* » (Davis, 1989, p. 320).

Les **conditions facilitatrices**, dans le contexte des S.I., correspondent au « *niveau de croyance d'une personne dans le fait qu'une infrastructure organisationnelle et technique existe pour l'aider dans son utilisation du système* » (Venkatesh *et al.*, 2003, p. 453). Il est à noter que ce construit est proche de la maitrise perçue du comportement utilisée dans la TPB.

La **motivation intrinsèque** est la perception que les utilisateurs accompliront une activité « *avec aucun stimulus autre que celui d'accomplir l'activité en elle-même* » (Davis *et al.*, 1992, p. 1112).

La **motivation extrinsèque** est la perception que les utilisateurs voudront réaliser une activité « *parce qu'elle est perçue comme un élément essentiel à l'atteinte des objectifs de résultats valorisés qui sont distincts de l'activité elle-même, comme l'amélioration du rendement au travail, de la rémunération ou des promotions* ». (Davis *et al.* 1992, p. 1112).

NB : L'UTAUT a renommé les divers construits ci-dessus. Le modèle reprend la facilité d'utilisation ('effort attendu'), l'utilité perçue ('performance espérée'), et les normes subjectives ('influence sociale') et ajoute les conditions facilitatrices afin d'expliquer l'intention comportementale et le comportement effectif. L'UTAUT a aussi inclus en variable modératrice l'utilisation volontaire qui, à la suite de mon étude qualitative, s'est révélée pertinente dans le contexte de la SSI.

# *Annexe 2 : Les principales études utilisant la PMT*

| Authors | Year | Sample | Determinants of ISS-related actions | | | | | | Dependent Variables | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Perceived Severity | Perceived Vulnerability | Response Efficacy | Self Efficacy | Response Cost | Social Influence | Behavioral Intention | Protective Actions | Supportive Actions |
| Workman et al. | 2008 | Employees, Large IT firm | + | + | + | + | + | | | X | |
| Gurung et al. | 2009 | Students | + | NS | + | + | NS | | | X | |
| Herath & Rao | 2009 | Employees, All Sizes | | NS | | + | | + | X | | |
| Lee & Larsen | 2009 | SME executives (60% IT) | + | + | + | + | + | + | X | X | |
| Ng et al. | 2009 | Employees, All sizes | NS | + | | + | | | | X | |
| Anderson & Agarwal | 2010 | Public users and students | + | | + | + | | NS | X | | |
| Johnston & Warkentin | 2010 | Faculty, staff and students | - | NS | + | + | | + | X | X | |
| Liang & Xue | 2010 | Students | + | + | + | + | + | | X | X | |
| Siponen et al. | 2010 | Employees, large companies | + | | NS | + | | + | X | X | |
| Lee | 2011 | Faculty | + | + | + | + | + | NS | X | X | |
| Ifinedo | 2012 | Employees, All sizes | - | + | + | + | NS | + | X | | |
| Vance et al. | 2012 | Administrative, City Govt | + | NS | - | + | + | | X | | |
| Yoon & Kim | 2013 | Employees, All Sizes | + | NS | + | + | | NS | X | | |
| Crossler & Belanger | 2014 | Students and citizens | + | - | + | + | NS | | | X | |
| Siponen et al. | 2014 | Employees, All sizes | + | + | NS | + | NS | + | X | X | |
| Boss et al. | 2015 | Students | + | NS | NS | NS | + | | X | X | |
| Johnston et al. | 2015 | Employees, City Govt | + | NS | + | + | | | X | | |
| Posey et al. | 2015 | Employees | + | | + | | NS | | | X | |
| Tu et al. | 2015 | Public users | + | | + | + | | + | X | | |
| Chen & Zahedi | 2016 | Individuals | + | + | + | + | | | | X | |
| Hanus & Wu | 2016 | Students | NS | NS | + | + | NS | | | X | |
| Tsai et al. | 2016 | eCommerce users | - | NS | + | - | + | + | X | | |
| Warkentin et al. | 2016 | Students | + | + | NS | + | | | X | X | |
| Barlette et al. | 2017 | SME CEOs | NS | NS | + | + | - | + | X | X | |
| Jansen & Schaik | 2017 | Individuals | + | NS | + | + | + | | | X | |
| Menard et al. | 2017 | Home users and employees | NS | NS | + | NS | NS | | X | | |
| Thompson et al. | 2017 | Home computer users | NS | + | NS | + | + | NS | X | X | |
| Aurigemma & Mattson | 2018 | Students | + | + | + | + | NS | | X | X | |
| Jansen & van Schaik | 2018 | Individuals | + | + | + | + | + | | X | | |
| Moody et al. | 2018 | Working professionals | NS | - | NS | - | | | X | | |
| Mwagwabi et al. | 2018 | Internet users | NS | NS | + | + | | | X | X | |
| Torten et al. | 2018 | IT Professionals | NS | + | + | + | - | | | X | |
| Verkijika | 2018 | Smartphone owners | + | + | NS | + | NS | | X | X | |
| Crossler et al. | 2019 | Students | + | NS | + | + | + | | X | | |
| Grimes & Marquardson | 2019 | Students | NS | NS | + | + | | + | X | | |
| Hina et al. | 2019 | Employees university | + | + | NS | + | | NS | X | | |
| Li et al. | 2019 | Employees, All sizes | NS | + | + | + | + | | | X | |
| Martens et al. | 2019 | Individuals | + | NS | + | NS | | + | X | | |
| Barlette & Jaouen (Protective | 2019 | SME CEOs | NS | + | + | + | | + | | X | |
| Barlette & Jaouen (Supportive | 2019 | SME CEOs | + | + | + | + | | + | | | X |

*NS: Non-significant;* **-** *: Opposite effect*

A jour au 1er mai 2020.
A noter, la récente méta-analyse réalisée par Cram *et al.* (2019) dans MISQ.

## *Annexe 3 : Article SIM 2008*

Barlette Y. 2008. Une étude des comportements liés à la sécurité des systèmes d'information en PME. *Systèmes d'Information et Management,* 13(4): 7-30.

## *Annexe 4 : Article SIM 2012*

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

## *Annexe 5 : Article SIM 2017*

Barlette Y., Gundolf K. & Jaouen A. 2017. CEOs' Information Security Behavior in SMEs: Does Ownership Matter? *Systèmes d'Information et Management*, 22(3): 7-45.

## *Annexe 6 : Article JOCM 2018*

Baillette P. & Barlette Y. 2018. BYOD-related innovations and organizational change for entrepreneurs and their employees in SMEs: the identification of a twofold security paradox, *Journal of Organizational Change Management*, 31(4): 839-851.

## *Annexe 7 : Article IJIM 2018*

Baillette P., Barlette Y. & Leclercq-Vandelannoitte A. 2018. Bring Your Own Device in organizations: Extending the reversed IT adoption logic to security paradoxes for CEOs and end-users, *International Journal of Information Management*, 43(December): 76-84.

# *Annexe 8 : Article JGIM 2020*

Baillette P. & Barlette Y. 2020. Coping Strategies and Paradoxes Related to BYOD Information Security Threats in France. *Journal of Global Information Management*, 28(2): 1-28.

NB : Cet article a été accepté le 19 décembre 2018. Le CNRS a déclassé JGIM en rang 3 dans son classement de novembre 2018, paru en février 2019…

## *Annexe 9 : Article SIM 2019*

Barlette Y. & Jaouen A. 2019. Information Security in SMEs: Determinants of CEOs' Protective and Supportive Behaviors. *Systèmes d'Information et Management*, 24(3): 7-40.

## *Annexe 10 : Article PPC 2020*

Barlette Y. & Baillette P. 2020. Big Data Analytics in turbulent contexts: towards organizational change for enhanced agility. *Production, Planning & Control*, 32. Published online August 2020.
(DOI: 10.1080/09537287.2020.1810755)

# *Annexe 11 : Article en cours de révision*

*Cet article a été soumis à EJIS puis Information & Management et rejeté au premier tour. Il a été resoumis, après modifications, à International Journal of Information Management, classé 3 CNRS et 2 FNEGE (I.F. 8,2).*

Barlette Y., Jaouen A. & Baillette P. (2020). Bring Your Own Device (BYOD) as a reversed IT adoption: Insights into Managers' Coping Strategies. *International Journal of Information Management.* Round 3.

## *Annexe 12 : Chapitre 2010*

Barlette Y. & Fomin V.V. 2010. The Adoption of Information Security Management Standards: A Literature Review, in Information Resources Management Association (Eds.). *Information Resources Management: Concepts, Methodologies, Tools and Applications:* 69-90, IGI Global, USA.

## *Annexe 13 : Chapitre 2014*

Barlette Y. & Jaouen A. **2014**. La relation entre le dirigeant et son expert-comptable en matière de gestion des informations. In Lecointre G. (Ed.), *Le Grand Livre de l'Economie PME 2015: 629-648*, Paris, Gualino.