Conception et mise en oeuvre d'une culture sécurité des systèmes d'information : le cas des PME

Olfa Ismail

THESE DE DOCTORAT DE

L'UNIVERSITE
DE BRETAGNE OCCIDENTALE

ECOLE DOCTORALE N° 597
Sciences Economiques et sciences De Gestion
Spécialité : « *Sciences de gestion* »

Par

Olfa ISMAIL

« Conception et mise en œuvre d'une culture sécurité des systèmes d'information : Le cas des PME »

Thèse présentée et soutenue à Brest , le 25 novembre 2021
Unité de recherche : Laboratoire d'Economie de de Gestion de l'Ouest (LEGO)

Rapporteurs avant soutenance :

Marc BIDAN, Professeur agrégé des Universités, Polytech Nantes et IAE de Nantes

Yves BARLETTE, Professeur PhD-HDR, Montpellier Business School

Composition du Jury :

Présidente : Sandrine BERGER-DOUCE, Professeure PhD-HDR, Ecole des Mines de Saint Etienne

Examinateurs : Hubert TONDEUR, Professeur agrégé des Universités, CNAM Paris

Marc BIDAN, Professeur agrégé des Universités, Polytech/ IAE de Nantes

Yves BARLETTE, Professeur PhD-HDR, Montpellier Business School

Dir. de thèse : Christian CADIOU, Professeur agrégé des université, IAE de Brest

Co-dir. de thèse : André MOURRAIN, Maître de conférences, IAE de Brest

L’Université de Bretagne Occidentale n’entend donner aucune approbation ni improbation aux opinions émises dans cette thèse : ces opinions doivent être considérées comme propres à leur auteur.

« N’écrivez pas seulement pour être compris. Ecrivez de façon à ce qu’il soit impossible que vous soyez mal compris »

Robert Louis Stevenson

Repose en paix chère FatHiya

Remerciements

Je n'oublierai jamais, le jour où j'ai demandé à **Christian Cadiou** de m'encadrer en thèse et de me signer la fiche pour demander une inscription. Il a signé la demande en me disant ''*Je vous fais confiance* Olfa''. J'espère avoir été à la hauteur de votre confiance. Je vous remercie énormément ainsi qu'**André Mourrain** de votre disponibilité, votre soutien et vos précieuses remarques qui m'ont permis d'aboutir à ce travail doctoral.

Je tiens également à remercier les professeurs, **Marc Bidan**, **Sandrine Berger-Douce**, **Hubert Tondeur** et **Yves Barlette** qui ont accepté de donner de leur précieux temps afin d'évaluer le présent travail. Leurs remarques, conseils et critiques me permettront de renforcer et de consolider mes futures recherches académiques.

Merci à **Kristen Cadiou** et à **Ivan Dufeu** pour leur participation à mon comité de suivi de thèse, ils m'ont tous deux permis de clarifier ma pensée parfois embrouillée et ont souvent fait preuve d'un enthousiasme communicatif à l'égard de ma prose.

Un grand merci également à **Yves Barlette**, professeur à Montpellier Business School, pour toute l'aide qu'il a su m'apporter, en ce qui concerne des références bibliographiques, des méthodes de recherche ou des remarques enrichissantes lors des conférences de l'AIM (Association Information et Management).

Je remercie infiniment les entreprises qui ont participé à mon étude et qui m'ont ouvert leur porte lors de mes interventions et lors des entretiens qualitatifs. Sans eux, cette thèse n'aurait pu voir le jour.

Mes remerciements vont aussi à **Patrick Gabriel** pour m'avoir accueillie au sein du laboratoire LEGO. Une mention spéciale pour **Cécile Morinière**, pour sa bienveillance à l'égard des doctorants, son écoute et sa disponibilité. Merci également à tous les doctorants qui contribuent à l'ambiance chaleureuse du laboratoire et plus particulièrement à **Sannae Ouaade** pour son hospitalité quand je n'avais plus de logement sur Brest.

Je remercie par ailleurs mes collègues de l'IAE de Brest, et en particulier **Marie-Noëlle Chalaye**, **Morgane Cavret** et **André Mourrain**, pour m'avoir donné l'opportunité d'exercer en qualité d'ATER (Attaché Temporaire d'Enseignement et de Recherche) et ainsi de finaliser cette thèse dans de meilleures conditions.

Je remercie aussi tous mes amis pour leur soutien et leurs encouragements pendant les moments les plus difficiles. Je pense particulièrement à **Houyam**, **Sirine**, **Aziza**, **Sabrine** et **Hatim**.

Je pense bien sûr à ma famille et particulièrement à mes parents **Afif** et **Noura** qui m'ont toujours incitée à aller au bout de mes rêves. Je remercie aussi mes deux sœurs et mes frères pour leurs encouragements et leur soutien indéfectible.

Je tiens également à remercier chaleureusement mon mari **Achraf** pour son soutien permanent et surtout pour sa grande patience, durant les longues soirées qu'il a passé seul devant la télévision quand j'étais plongée dans le travail de ma thèse.

Cette liste n'est pas exhaustive et je remercie tous ceux et celles qui me connaissent et qui ont cru en moi.

Sommaire

Terminologie

Acronyme/sigle	Signification
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CCI	Chambre de Commerce et de l'Industrie
CS	Culture Sécurité
CSSI	Culture Sécurité des Systèmes d'Information
Clusif	Club de la Sécurité de l'Information Français
CPME	Confédération des Petites et Moyennes Entreprises
CMMI	Capability Maturity Model Integrated
Cnil	Commission nationale de l'informatique et des libertés
CobiT	Control Objectives for information and technology
COSO	The Committee of Sponsoring Organizations of the Trendway Commission
DPO	Data Protection Officer
ERP	Enterprise Resource Planning
ETI	Entreprises à Taille Moyenne
GSI	Gouvernance des Systèmes d'Information
GREPME	Groupe de Recherche en Economie et Gestion des Petites et Moyennes Entreprises
HAIS-Q	The Human Aspects of Information Security Questionnaire
ISCA	Information Security Culture Assessment
ISACA	Information Systems Audit and Control Association
ISTAAP	Information Security Training And Awareness Approach
ISO	International Organization for Standardization
INSEE	Institut National de la Statistique et des Etudes Economique
ITIL	Information Technology Infrastructure Library
MISSTEV	Model for Information Security Shared Tacit Espoused Values
OECD	Organisation de Coopération et de Développement Economiques
PRA	Plan de Reprise d'Activité
PCA	Plan de Continuité d'Activité
PME	Petite et Moyenne Entreprises
PMT	Protection Motivation Theory
RI	Recherche Intervention
RH	Ressources Humaines
RGPD	Règlement Général sur la Protection des données
RTPO	Recovery Time and Point Objectives
R&D	Recherche et Développement
RSI	Responsable su Système d'Information
RSSI	Responsable de la Sécurité des Systèmes d'Information
SETA	Security Education Training Awareness
S.S.I.I	Société de Services et d'Ingénierie en Informatique
SSI	Sécurité des Systèmes d'Information
SMSI	Système de Management de la Sécurité de l'Information
SARL	Société Anonyme à Responsabilité Limité
SAS	Société par Actions Simplifiée

SASU	Société par Actions Simplifiée Unipersonnelle
TIC	Technologies de l'Information et de la Communication
TRA	Theory of Reasoned Action
USB	Universal Serial Bus
UNESCO	United Nations Educational, Scientific and Cultural Organization

Index des figures

Index des tableaux

Index des matrices

INTRODUCTION GÉNÉRALE

« *Lundi matin, on arrive à nos bureaux et on voit un écran noir.* » C'est la douche froide pour le patron et les 20 salariés de LVH électronique, une PME bretonne. La PME se retrouve au chômage technique et a perdu 30 000 € en février 2019. En cause, « *un mail avec une pièce-jointe contenant un virus qui a pris la main sur nos serveurs* », se rappelle le patron[1].

Les systèmes d'information des entreprises sont de plus en plus ouverts aux acteurs externes (fournisseurs, clients, partenaires, etc.). Les techniques comme l'e-commerce, les réseaux locaux, l'e-mail, l'Intranet et l'Extranet amènent les entreprises à gérer l'accessibilité de leurs systèmes d'information. En contrepartie de cette ouverture, la vulnérabilité des entreprises aux incidents va augmenter, et peut même conduire à la liquidation telle que le cas de la société Lise Charmel[2] qui était mise en redressement judiciaire le 27 février 2020 suite à une attaque par rançongiciel[3].

En plus, aujourd'hui, les outils nécessaires aux pirates sont de plus en plus accessibles en ligne et il existe un échange constant d'informations et de savoir-faire au sein de la communauté des pirates pour rendre ces attaques de plus en plus efficaces.

Notre recherche trouve son origine sur le constat de l'exposition des entreprises au risque de fraude et que le nombre de fraudes se traduit chaque année par des préjudices s'élevant à des milliards d'euros, en particulier pour les hôpitaux, les banques et les entreprises. Notre travail doctoral interroge en ce sens la manière ou les méthodes à mettre en place pour minimiser les risques et les fraudes liés aux systèmes d'information. Dans cette introduction, nous allons évoquer l'enjeu stratégique de la sécurité des systèmes d'information **(1)** et l'intérêt d'étudier la dimension culturelle de la sécurité des systèmes d'information **(2)**, la problématique générale et la question de recherche **(3)**, et ensuite, nous soulignerons les visées de la recherche **(4)**, le positionnement épistémologique choisi **(5)**, et nous terminerons par le plan mis en œuvre **(6)**.

[1] Source : https://www.leparisien.fr/ par Cyril Peter, le 10/12/2019
[2] Source : https://www.ouest-france.fr/ le 04/03/2020
[3] D'après l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), le rançongiciel ou ransomware consiste en l'envoi à la victime d'un logiciel malveillant qui chiffre l'ensemble de ses données et lui demande une rançon en échange du mot de passe de déchiffrement.

1. La sécurité des systèmes d'information : un enjeu stratégique

Nous remarquons une contradiction apparente entre, d'une part, la nécessité pour les entreprises de protéger leurs systèmes d'information et, d'autre part, la nécessité de s'adapter à l'évolution et l'ouverture de leurs environnements.

Tout d'abord, il faut comprendre que l'information est une composante essentielle à toute entité, c'est un flux de données vitales pour la bonne marche de chaque entreprise. Nous pouvons comparer l'importance de l'information au système cardio-vasculaire d'un être vivant car l'information est au cœur de toutes activités stratégiques et opérationnelles, qui permet à une entreprise d'atteindre ses objectifs. Pour Lesca et al (2010) « *L'information c'est vital pour l'entreprise, qu'elle soit grande ou petite* ».

Chaque entreprise consacre un temps, un effort et un coût important pour collecter et gérer une information dite « stratégique ». Dans ce cas, nous pouvons introduire la notion de la « veille stratégique », qui est un processus systématique, continu, éthique et légal, de collecte, d'analyse, de traitement et de diffusion de l'information, celle-ci visant à aider les gestionnaires, la haute direction ou l'organisation dans son ensemble, à prendre de meilleures décisions et à alimenter la réflexion stratégique, grâce à une meilleure compréhension de l'environnement externe et interne (Bergeron & Hiller 2002 ; Guechtouli 2014 ; Drevon et al 2018).

L'information est non seulement générée à l'intérieur d'une entreprise, mais elle est aussi échangée avec l'extérieur de l'entité. Son rôle est d'aider à la réflexion, à la construction d'un savoir-faire et à la prise de décision. Pour Achchaba et Harrizi (2013), l'information est devenue un facteur déterminant de compétitivité, d'avantage concurrentiel et d'innovation ; c'est l'élément nouveau qui fait la différence de nos jours. Car, avec une économie qui se mondialise où la concurrence s'accroît, et où les organisations cherchent à offrir davantage de produits et de services aux clients, l'information est de plus en plus une variable stratégique essentielle.

Selon Martinet et Marty, (2001), « *donner de la valeur concurrentielle à l'information* » est une des caractéristiques principales de l'intelligence économique que nous considérons une notion très important à souligner. Cette notion se définit comme « *un système collectif d'acquisition de production et de transformation de l'information en connaissances utiles permettant à l'entreprise d'améliorer ses processus de décision, son image, sa capacité d'influence, de créer de la valeur, de saisir des opportunités, de renforcer sa compétitivité, d'innover, de détecter*

des menaces, de prévenir des risques, d'assurer la sécurité et la sureté de ses membres et de ses partenaires, d'accroître et de protéger ce patrimoine. » (Besson et Possin, 2004).
Bournois et Romani (2000) ont analysé les similitudes entre l'intelligence économique et la sécurité des systèmes d'information. Deux types de rapports apparaissent de leur analyse : la sécurité des S.I. englobe l'intelligence économique; l'un et l'autre sont en coordination étroite. La sécurité des S.I. va permettre de protéger cette « valeur concurrentielle » de l'information ainsi que la compétitivité de l'entreprise obtenue grâce à ces informations.

Rappelons maintenant la notion du système d'information qui est définie selon Reix (2002) comme « *Ensemble organisé de ressources : matériel, logiciel, personnel, données, procédures… permettant d'acquérir, de traiter, de stocker des informations (sous forme de données, textes, images, sons, etc.) dans et entre des organisations* ».

Donc la notion du système d'information est étroitement liée à la notion de l'information, puisque le système d'information c'est le système qui va capter, traiter et stocker les informations.

Pour Laudon et al (2010), les systèmes d'information sont indispensables dans la gestion quotidienne des entreprises et ils sont essentiels pour la réalisation des objectifs stratégiques des entreprises. En plus, les enjeux liés aux systèmes d'information « *sont d'importance, compte tenu du rôle qu'ils jouent dans le fonctionnement efficient des organisations et leur potentiel compétitif* » (Kefi et Kalika, 2004).

Selon une étude faite par Clusif[4] (2020) toutes les entreprises interrogées tous secteurs confondus et quelle que soit leur taille confirment, que le système d'information est perçue comme stratégique.

Donc la protection de ces systèmes d'information s'avère un enjeu majeur pour les organisations afin de protéger leurs informations et afin de garantir leur pérennité. Au niveau de littérature, une étude récente de Moon et al (2018), montre que le niveau d'efficacité de la sécurité des SI avait une influence positive sur la performance organisationnelle, y compris la performance axée sur les processus financiers et opérationnels. Une autre étude de Dagorn et Poussing (2012) réalisée auprès de 120 grandes entreprises luxembourgeoises, montre que 95% des organisations pensent pouvoir retirer un avantage concurrentiel (bénéfices très importants ou

[4] Club de la sécurité de l'information français

importants) de la gouvernance de la sécurité de l'information et 75% d'entre elles sont engagées dans la démarche.

2. La sécurité des systèmes d'information : La transformation culturelle

D'un côté, les organisations investissent dans la sécurité de leurs infrastructures informatiques, et mettent en place des mesures techniques, et d'un autre côté un certain nombre d'études ont appliqué diverses techniques pour motiver les employés à adopter des intentions et des comportements sûrs, malgré ces efforts, les employés restent le «maillon faible» de la sécurité informatique organisationnelle (Silic et Lowry, 2020).

D'après une étude faite par Clusif en 2020, les incidents les plus fréquemment signalés ont eu pour cause des erreurs d'utilisation (de saisie, d'exploitation du système, etc.) et des vulnérabilités qui viennent de l'intérieur de l'entreprise.

Donc nous constatons qu'il y a avant tout, des problèmes de comportement humain, où les gens n'ont pas la compréhension de la menace ni des risques. S'ajoutent à ce constat, les résultats d'autres études et recherches qui montrent qu'une grande part des pertes provoquées par des atteintes à la sécurité de l'information a pour origine les propres collaborateurs de l'entreprise (Wang et al. 2015), agissant de façon volontaire (Willison et Warkentin, 2013) ou involontaires (Guo et al., 2011).

La sécurité de l'information doit donc se situer dans une perspective d'amélioration continue et constitue un des fondements de la culture organisationnelle (Barlette, 2012). À cet égard, elle nécessite une mobilisation des salariés (Johnston et al. 2015).

Schein (1985) a postulé que la culture organisationnelle est puissante et souvent force inconsciente qui établit les comportements des employés. Ainsi, la relation entre culture organisationnelle et comportements des employés doit être prise en compte lors de la mise en œuvre des pratiques de sécurité, car elle a un impact sur le comportement des employés dans les organisations (Thomson et al, 2006).

La culture de la sécurité des SI doit être considérée dans le cadre du programme de sécurité des SI pour orienter le comportement des employés. Une telle culture peut contribuer à la protection de l'information et minimiser le risque que pose le comportement des employés. (Martins et Da Veiga, 2015).

Parsons et al, (2015), montrent qu'il existe une relation significative et positive entre les décisions qui concernent la sécurité des informations et la culture sécurité des informations. De telle sorte que l'amélioration de la culture sécurité de l'information d'une organisation aura une influence positive sur les comportements des employés, ce qui peut atténuer les risques liés aux systèmes d'information. Par conséquent, la création d'une culture de la sécurité de l'information est nécessaire pour une gestion efficace de la sécurité des systèmes d'information.

Pour cela, nos préoccupations vont s'orienter désormais vers la **culture sécurité** dans le domaine de la sécurité des systèmes d'information.

3. La sécurité des systèmes d'information en PME : Problématique et questions de recherche

Notre démarche, nous a permis de soulever d'un côté l'importance et l'actualité des questions de la **sécurité** et d'un autre côté l'intérêt que représentait l'étude de la **culture sécurité**. Il nous reste de préciser que notre recherche se situe dans le cadre des PME. Alors, pourquoi les PME représentent-elles un champ d'études important ?

Premièrement, dans la dernière enquête du Clusif (2020), il a été prouvé que la maturité des grandes entreprises en matière de sécurité de l'information est meilleure par rapport à celle des plus petites. Selon une enquête de la CPME[5] (2019), 41 % des entreprises interrogées de 0 à 9 salariés et 44% des entreprises de 9 à 49 salariés ont déjà subi une ou plusieurs attaques ou tentatives d'attaques informatiques.

La principale raison de ces attaques est que les PME ont des défenses plus faibles que les grandes entreprises (manque d'expertise, défenses de sécurité datées, sous-traitance à des entreprises non qualifiées), et que les PME peuvent également servir de moyen d'atteindre les données des plus grandes organisations. Cependant, malgré cette réalité, de nombreuses PME estiment toujours qu'elles ne sont pas vulnérables aux cyberattaques en raison de leur petite taille et de leurs actifs limités.

Deuxièmement, car peu de travaux ont étudié la sécurité dans les PME (Kyobe, 2008, Barlette et al 2017), même si les PME font face à des problèmes plus importants que ceux rencontrés par de plus grandes entreprises, citant par exemple les problèmes de recrutement de personnes qualifiées dans les TIC (Pritchard, 2010), et du manque de sensibilisation à la sécurité des

[5] Confédération des Petites et Moyennes Entreprises

systèmes d'information (Rees, 2010). Les PME ne disposent ni des ressources matérielles et techniques (Labodi et Michelberger, 2010) ni des ressources humaines et financières (Lee et Larsen, 2009) pour bien gérer leur sécurité des systèmes d'information.

Bien que des études démontrent l'inquiétude des PME quant aux difficultés liées au développement d'une culture de la sécurité de l'information (Taylor et Murphy, 2004), le fait est que la culture sécurité a de sérieux problèmes concernant sa mise en œuvre dans les PME (Hutchinson et al, 2014).

Selon (Dojkovski et al, 2006 ; Hutchinson et al, 2006), les PME sont, par rapport aux grandes organisations, particulièrement enclines à rechercher une culture de la SSI. C'est pour les raisons suivantes :

-Les PME ne disposent généralement pas de politiques procédurales et ne définissent pas non plus les responsabilités des utilisateurs de leurs systèmes d'information (Helokunnas et Iivonen, 2004).

-Par rapport aux grandes entreprises, les PME sont plus sensibles aux influences nationales, telles que les modifications de la législation (Warren, 2003).

Kuusisto et Ilvonen (2003) parviennent à la conclusion qu'il n'existe pas de réglementation appropriée pour la gestion de la sécurité dans les PME, et qu'il existe principalement un besoin de modèles valides, qui permettront de renforcer la culture de la sécurité dans les PME (Santos-Olmo et al, 2016). Nous pouvons souligner que plusieurs cadres de gestion de la sécurité pour le développement d'une culture de la SSI ont été développés, mais ils ont tendance à être orientés vers les grandes organisations. Selon Hutchinson et Warren (2006), et Dojkovski et al, (2006), les cadres pour les PME devraient être basés sur l'étude de leurs besoins réels afin d'identifier et de développer un cadre qui leur est spécifiquement destiné.

Les PME présentent donc de nombreux intérêts théoriques : Elles ont des spécificités, en regard des TIC et de la sécurité des TIC, qui justifient une meilleure compréhension des problématiques sécuritaires. De plus, il nous semble que ces problématiques soient plus intéressantes au niveau des PME, ce qui nous dirige à axer notre recherche sur ce type d'entreprises.

Le champ de la sécurité des SI, la dimension culturelle de la sécurité des SI et le champ des PME comme terrain de recherche, nous invitent à poser notre question générale suivante :

« Comment insuffler une culture sécurité des systèmes d'information en PME? »

Tout au long de notre travail, nous allons apporter les éléments théoriques, conceptuels ainsi que pratiques pour répondre à cette question centrale de notre recherche.

4. Visées de la recherche

Les résultats avancés ainsi que les différentes contributions théoriques et managériales de la présente recherche, sont indispensables pour expliquer, piloter et accompagner les pratiques dans le cadre de la sécurité des systèmes d'information dans les PME et pour expliquer, conceptualiser et améliorer la culture sécurité des utilisateurs.

4.1) Visées académiques

Le modèle conceptuel de cette recherche fait l'emprunt de l'approche systémique de modélisation. Cette approche contribue à prendre en compte, pour le premier niveau d'analyse, l'ensemble des facteurs influençant la culture sécurité des utilisateurs des systèmes d'information, pour le second niveau d'analyse, les déterminants de cette culture ; et enfin pour le troisième niveau d'analyse, le résultat qui est les comportements de sécurité. L'importance de cette modélisation systémique se manifeste par la généralisation de la problématique d'amélioration de la culture sécurité, mais aussi par son aptitude à mettre en place un diagnostic global du contexte de la sécurité des systèmes d'information. Elle vise à contribuer, en ce sens, à l'identification d'un certain nombre d'actions à mettre en œuvre pour améliorer le niveau de la sécurité des systèmes d'information dans la PME.

Plusieurs cadres de gestion de la sécurité pour le développement d'une culture de la sécurité des systèmes d'information ont été développés. nous aurons l'occasion de les mentionner tout au long de cette recherche, mais ils ont tendance à être orientés vers les grandes organisations. Santos-Olmo et al, (2016) affirment qu'il existe un besoin de modèles valides qui permettront de renforcer la culture de la sécurité dans les PME. Cette recherche va tenter de combler cette

lacune, à travers la proposition d'un modèle spécifique aux PME qui permet l'évaluation et l'amélioration de la culture sécurité.

4.2) Visées managériales

Qui renvoient aux résultats relatifs à l'influence des différents facteurs contextuels sur la culture sécurité des utilisateurs des systèmes d'information et en conséquence, les comportements de sécurité de ces utilisateurs, ainsi qu'aux actions à mettre en place pour améliorer la culture et les comportements proposés aux PME.

Les résultats relatifs aux PME étudiées mettent en évidence l'influence notable des déterminants contextuels sur la culture et les comportements de sécurité des utilisateurs à l'égard des systèmes d'information, sur leurs croyances ainsi que sur leurs manières d'agir pour protéger les systèmes d'information de leurs entreprises. Les résultats de cette recherche offrent la possibilité aux dirigeants des PME de mieux connaître les facteurs sur lesquels agir pour améliorer la culture de sécurité des salariés ainsi que leurs comportements pour garantir une meilleure sécurité de leurs systèmes d'information.

Plus généralement, ces résultats sont à même d'offrir la possibilité de mieux orienter les PME voulant la mise en place des mesures ou des programmes d'amélioration de la sécurité des systèmes d'information centrée sur la dynamique du changement, en les assistant à accréditer un dispositif d'accompagnement pour améliorer la culture et les comportements des utilisateurs. En plus, nous offrons un cadre qui permet d'évaluer le niveau de la sécurité des systèmes d'information au sein de la PME, y compris les niveaux de la culture et des comportements pour pouvoir ensuite définir les actions correctives requises pour atténuer les faiblesses et améliorer, par-là, le niveau de la sécurité des systèmes d'information.

5. Positionnement épistémologique de la recherche

Le positionnement épistémologique reflète la vision du monde sur laquelle repose une recherche (Perret et Séville, 2007). De cette vision dépendent les questions de recherche, la démarche de recherche et le type de connaissances produites. L'épistémologie peut être définie comme « *une activité réflexive qui porte sur la manière dont les connaissances sont produites*

et justifiées » (Thietart et al. 2014). Tout travail de recherche implique dès lors de s'inscrire dans un paradigme épistémologique.

Notre recherche se positionne dans le paradigme **interprétativiste**, puisque nous nous inscrivons dans une approche qui vise à comprendre la réalité, et ce paradigme adopte une démarche basée sur la compréhension plutôt que l'explication. Les connaissances générées par ce paradigme sont principalement d'ordre descriptif, dans la mesure où « *la construction de connaissance vise d'abord à comprendre les significations que les différents sujets participant à une même situation donnent à cette situation* », Gavard-Perret et al. (2012).

Notre mode de raisonnement est **abductif** dans la mesure où la recherche alterne questionnements théoriques et études empiriques dans une optique résolument exploratoire. L'idée générale consiste alors à construire un cadre conceptuel à partir d'éléments théoriques et empiriques. Afin d'étudier la culture sécurité des SI en profondeur et d'une vision systémique, nous avons mobilisé une méthodologie **qualitative** à travers des études de cas, qu'elle permet d'expliquer les mécanismes psychologiques qui peuvent former la culture sécurité de l'utilisateur des SI.

6. Plan de la recherche

Le plan choisit pour problématiser notre travail et répondre à la question de recherche est initié par un chapitre préliminaire et articulé autour de deux parties constituées chacune de deux chapitres :

Le **chapitre préliminaire** vise à justifier l'objet de recherche et affiner la problématique de recherche à travers la conduite d'une intervention au sein d'une PME. Cette étape préliminaire, nous a permis d'aller plus loin dans la littérature et d'étudier ensuite notre objet dans son ensemble et d'une vision plus systémique.

Dans la **première partie**, nous examinons la littérature en profondeur. Ensuite, nous construisons un modèle conceptuel de la culture sécurité des SI. L'apport de cette partie est avant tout conceptuel.

Le **premier chapitre** présente le cadre théorique de la recherche. Il situe, dans un premier lieu, le contexte général de cette étude qui consiste en une synthèse, d'une part, de la notion de «la culture sécurité des utilisateurs des systèmes d'information», et les recherches dans le contexte des PME, et, d'autre part, « les comportements relatifs à la sécurité », et les recherches en PME.

Le premier chapitre développe, dans un second lieu, les actions à mettre en place pour assurer la sécurité des systèmes d'information.

Le **deuxième chapitre** justifie le choix et la structure du modèle conceptuel qui se base sur une approche systémique composée de trois niveaux, définit les concepts correspondant à chacun des trois niveaux d'analyse, et définit les orientations de recherche qui caractérisent les relations étudiées entre les différents niveaux d'analyse du modèle.

La **deuxième partie** nous permet de présenter plus en profondeur la démarche de recherche, de confronter notre modèle conceptuel à la réalité du terrain et de discuter les résultats obtenus.

Le **troisième chapitre** relève d'une analyse qualitative. Il se situe dans une démarche de recherche et trouve une application dans huit cas de PME. Nous présentons une typologie des PME étudiées ainsi qu'une typologie des utilisateurs des SI interrogés.

Le **quatrième chapitre**, nous permet d'examiner nos orientations de recherche définies au niveau de la première partie et de discuter nos résultats de recherche.

La **conclusion générale** de la recherche établit une synthèse des majeures contributions de cette recherche, aussi bien théoriques, méthodologique, que managériales. Elle reconnaît, en définitive, les limites de cette étude et avance des voies futures de recherche sur la sécurité des systèmes d'information et plus particulièrement les volets culturel et comportemental.

La figure (page suivante) schématise le plan de recherche que nous venons de présenter :

Figure 1 : Plan de la recherche

Introduction générale

Chapitre préliminaire : L'intentionnalité de la recherche

Partie I :

Conception d'une culture sécurité des SI en PME : vers un modèle conceptuel

Chapitre 1 : La culture sécurité des systèmes d'information dans les PME: Une revue de littérature

1) État des lieux de la connaissance
2) Les comportements liés à la sécurité
3) Les actions à mettre en place pour sécuriser les systèmes d'information

Chapitre 2 : Construction d'un modèle conceptuel adapté à la PME et orientations de recherche

1) Précisions des concepts du modèle
2) Modèle conceptuel et orientations de la recherche

Partie II :

Déploiement du modèle conceptuel de la culture sécurité: Méthodologie et résultats

Chapitre 3 : Etudes de cas: pratiques de PME en sécurité des SI

1) Positionnement épistémologique et méthodologique
2) Vers une typologie des cas étudiés : analyse des résultats

Chapitre 4 : Examen des orientations de recherche et discussion des résultats

1) Retour sur les orientations de recherche et discussion des résultats
2) Retour sur le modèle conceptuel

Conclusion générale

Chapitre préliminaire : L'intentionnalité de la recherche

Avant d'aborder de plain-pied le sujet de notre thèse, à savoir, la culture sécurité des systèmes d'information dans les PME, il est utile de présenter dans ce chapitre préliminaire le fil conducteur qui nous a amené à l'identification de notre objet de recherche qui se situe à l'intersection de trois champs : le champ de la sécurité des systèmes d'information, le champ de la culture, et le champ de la PME.

Au cours de l'année universitaire 2016/2017, nous avons effectué un mémoire de recherche dans le cadre d'un mastère de recherche à l'Université de Bretagne Occidentale (UBO), qui porte sur la compréhension des comportements en matière de sécurité des systèmes d'information et plus particulièrement nous avons étudié la vision des dirigeants sur le sujet. Tout au long du travail pour ce mémoire, nous avons mis en lumière l'importance de la sensibilisation à la sécurité des SI afin de réduire le risque lié au facteur humain (dirigeants, responsables et salariés) sur le SI de l'entreprise.

Parmi les résultats obtenus par notre étude terrain effectuée en interrogeant huit dirigeants de PME, nous avons identifié les motivations et les freins à une mise en place d'une politique de sensibilisation (y compris une formation) à la sécurité des SI, et parmi les freins identifiés, nous avons trouvé le manque de ressources financières et le manque de temps, ce qui a été en cohérence avec la littérature qui affirme que les PME ne disposent ni des ressources matérielles et techniques (Labodi et Michelberger, 2010) ni des ressources humaines et financières (Lee et Larsen, 2009) pour gérer correctement leur SSI.

En effet, la plupart des organisations, et surtout les PME, ont des problèmes en matière de sécurité des informations. D'un côté, le manque de sensibilisation des salariés va entraîner des erreurs d'utilisation des logiciels, de la malveillance et une mauvaise application des politiques de sécurité, et d'un autre côté, l'insensibilité des dirigeants d'entreprises aura une incidence sur la mise en œuvre de ces politiques de sécurité et sur les investissements essentiels.

Un des principaux problèmes posés lors de la mise en place de politiques de sécurité est le contournement de ces politiques par les employés. Ceci peut être conséquence d'un problème

de communication qui provient d'un degré de différence important entre les acteurs. D'ailleurs, Schein (1996) explique que les « *chocs culturels* » qui peuvent se développer dans les organisations sont souvent la conséquence d'un manque de communication entre trois catégories de personnes : les managers, les employés et les ingénieurs.

En réalité, beaucoup d'entreprises, même si elles se disent sensibilisées, ne passent pas à l'action, c'est pourquoi une sensibilisation des dirigeants pourrait permettre d'améliorer leur implication dans la sécurisation de leur entreprise. Selon Pipkin (2000), un programme de sensibilisation doit être accessible à toute personne, interne ou externe, qui aura accès aux informations.

Revenons sur les résultats de notre étude précédente. Parmi les dirigeants interrogés, un seul dirigeant, était très motivé à mettre en place une sensibilisation à la sécurité dans son entreprise : *« Oui, je voulais bien mettre en place une politique de sensibilisation pour les salariés, telle que des affiches, des clauses dans les contrats »* (Dirigeant A).

À la fin de notre mémoire de recherche, nous avons proposé au dirigeant A, d'effectuer une intervention au sein de son entreprise pour sensibiliser et former les salariés à la sécurité des SI. Nous avons entrepris cette démarche, dans un objectif de décrire, expliquer et transformer l'objet de recherche pour mieux le connaître (Savall, 1978 ; Moisdon, 1984 ; Avenier, 1989 ; Savall et Zardet, 1996, 2004 ; David, 2000 ; Plane, 2000), surtout que nous avons été en phase de préparation de notre projet de thèse et cette étape nous a permis de creuser plus sur le sujet de la sécurité des SI au sein de la PME et d'affiner notre problématique de recherche. Dans le titre suivant nous allons développer les étapes de cette intervention réalisée.

1. Intervention au sein d'une PME

Avant de décrire le déroulement de cette intervention, nous nous sommes inspirés de la démarche d'une recherche intervention, qui nous paraît intéressant de la définir et de montrer le lien entre ce type de recherche et notre expérience professionnelle sur le terrain.

1.1 Qu'est-ce que la recherche intervention (RI)?

La recherche intervention ou RI a connu un essor récent dans les sciences de gestion, même s'il convient de souligner qu'elle s'inscrit dans un courant de pensée ancien qui a été initié par Taylor et al (1970), Lewin (1959), l'école socio-technique (1983), et, ensuite, le développement

des organisations (1975). Ce courant de pensée a mis l'accent sur le rôle des problèmes issus du terrain, comme source privilégiée de production des connaissances. Mais, au sens propre du terme, la RI elle est apparue en France dès les années 1970, à l'initiative de l'ISEOR[6] (Savall, 1977, 1979 ; Savall et Zardet, 1984) et du CGS (Centre de Gestion Scientifique de l'Ecole des Mines de Paris).

Selon Moisdon, (2010), la RI s'appuie sur l'idée qu'il n'est possible d'appréhender le fonctionnement d'une organisation « *qu'en y pénétrant, en y intervenant et, par conséquent, en la modifiant* ». Elle s'oppose aux recherches de nature « contemplative », en visant l'appropriation et l'utilisation, par les praticiens de l'entreprise, d'une partie des connaissances co-produites avec le chercheur. Elle vise à donner du sens, en allant au-delà de l'explication et la théorisation (Royer et al, 2009).

Cappelletti, (2010), définit cette méthode comme suit : « *La recherche intervention vise* […] *la formalisation et la contextualisation du changement. Elle cherche à transformer effectivement l'organisation dans ses structures et ses comportements* […] ».

Dans ce type de recherche, le chercheur vise deux objectifs indissociables : accompagner l'entreprise dans une action délibérée de changement et produire de la connaissance à partir de l'observation des transformations réalisées. La recherche intervention est donc : une logique intentionnelle, une visée transformatrice, un projet de changement délibéré (Lewin, 1947) d'une situation donnée (Le Moigne, 1990).

La RI s'appuie, à la manière des anthropologues, sur une immersion dans l'organisation en vue de conduire une intervention, c'est-à-dire d'accompagner ou de susciter une transformation de l'organisation. L'objectif du chercheur intervenant est de produire des résultats qui s'intègrent dans une interaction avec les acteurs de terrain. C'est en ce sens qu'on parle de démarches interactives (Girin, 1986). Par ailleurs, les conclusions sont fondées sur « *l'intime conviction du chercheur, qui se retrouve dans l'arène pour éprouver lui-même les champs de force qui traversent l'organisation* » (Moisdon, 2010).

La RI constitue ainsi une forme spécifique de recherche en sciences de gestion. Elle vise à produire des connaissances qui seront à la fois utiles aux acteurs de terrain pour les aider à résoudre leurs problèmes concrets et intéressantes pour les sciences de gestion. En ce sens-là,

[6] Institut de Socio-Économie des Entreprises et des Organisations fondé en 1975 par Henri Savall, professeur émérite à l'université Lyon III Jean Moulin.

RI s'apparente à ce que Glaser et Strauss (1967) ont appelé des théories intermédiaires fondées "Grounded Theories" c'est-à-dire, des théories qui reposent sur un va-et-vient, un dialogue permanent à un double niveau : d'une part, avec les problèmes nés du terrain, et d'autre part, avec les théories générales en vigueur dans les sciences de gestion.

Ce type de recherche qui consiste à partir du terrain pour produire des connaissances à la fois opératoires et théoriques tend à valoriser une vision renouvelée des sciences de gestion comme relevant d'une ingénierie spécifique dans la lignée des travaux de Lemoigne (1993) ou de Martinet et al (1997).

Pour Aggeri (2016), la RI ne vise pas à tester des hypothèses théoriques qui auraient été identifiées en amont, mais bien d'engager une exploration afin de mieux caractériser le problème en jeu et d'identifier des pistes de réflexion ou d'instrumentation. Il est difficile, dans de telles recherches, d'établir au début du processus et avant d'aller sur le terrain une revue de littérature entièrement pertinente, les théories existantes étant sans cesse revisitées grâce aux matériaux empiriques (David, 2000).

Dans cette optique, nous qualifions notre intervention sur le terrain comme une recherche très proche d'une recherche intervention, en s'inscrivant dans une démarche dialectique, entre théorie et pratique pour favoriser la compréhension, l'intelligibilité. (Saint-Jean et al, 2014).

1.2 Les cinq principes méthodologiques de la recherche intervention

Du point de vue méthodologique, la recherche intervention s'articule autour de cinq principes selon Hatchuel, A. (1994b) : le principe de rationalité accrue, le principe d'inachèvement, le principe de scientificité, le principe d'isonomie et le principe des deux niveaux d'interaction :

Le principe de rationalité accrue indique que le chercheur intervenant doit *« favoriser une meilleure adéquation entre la connaissance des faits et les rapports qu'ils rendent possibles entre les hommes »*. Il s'agit non pas de mettre en place un dialogue entre les acteurs ou d'apporter de l'extérieur des connaissances d'experts, mais de penser la mise en comptabilité de relations et de savoirs nouveaux.

Le principe d'inachèvement indique qu'il est impossible de spécifier à l'avance le chemin et les résultats d'une recherche intervention : c'est le but du dispositif que de générer des connaissances nouvelles de nature à faire évoluer l'organisation.

Le principe de scientificité correspond à l'idéal de vérité. Le chercheur doit avoir en permanence une attitude critique par rapport aux faits. Le chercheur n'est pas « l'expert des experts » mais doit s'interroger sur les conditions de validation des savoirs mobilisés au cours de l'intervention.

Le principe d'isonomie indique que *« l'effort de compréhension doit s'appliquer également à tous les acteurs concernés »*. L'intervention elle-même doit donc se traduire concrètement par la mise en place d'un système d'échanges entre acteurs qui respecte à la fois recherche de vérité et démocratie.

Le principe des deux niveaux d'interaction indique que la recherche intervention suppose à la fois un dispositif d'intervention et une démarche de connaissance. Dans le dispositif d'intervention, la relation du chercheur aux autres acteurs n'est pas fixée à l'avance. La démarche de connaissance est une démarche activatrice, dans laquelle le chercheur stimule la production de nouveaux points de vue.

Au total, *« l'intervention n'est pas seulement l'exploration d'un système mais la production de savoirs et de concepts qui permettent de penser les trajectoires dans lesquelles un collectif pourrait s'engager »* Hatchuel, A. (1994b).

1.3 Déroulement de l'intervention

Notre intervention s'est déroulée à partir du début octobre 2017. Nous avons recontacté le dirigeant de l'entreprise A qui a déjà été motivé pour une intervention au sein de sa PME dans le but d'améliorer le niveau de la sensibilité à la sécurité et plus généralement de travailler sur des pistes qui peuvent améliorer la sécurité des SI de son entreprise. Nous allons présenter et décrire ci-dessous le processus de notre intervention qui se déroule en quatre étapes essentielles :

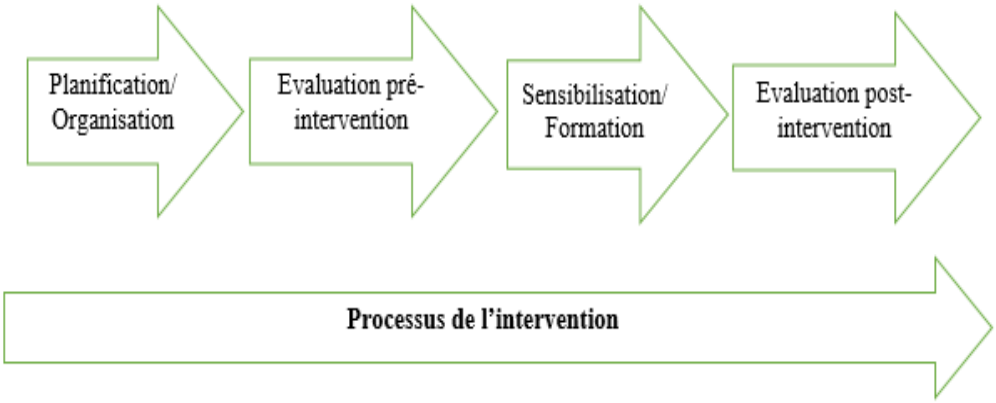


Figure 2 : Les étapes du déroulement de l'intervention

Etape 1 : Planification et organisation de l'intervention

Dans cette première étape, nous avons effectué un échange avec le dirigeant de la PME afin d'identifier les besoins et les éléments nécessaires à mettre en place pour améliorer la sécurité et sensibiliser les utilisateurs du SI.

Nous avons identifié trois outils clés à mettre en place à savoir : une sensibilisation, une formation et une charte de sécurité. Nous, nous considérons la sensibilisation et la formation comme les prémisses d'une mise en place de la sécurité des SI. Kruger et Kearney, (2006), déclarent que : « *L'indifférence et l'ignorance vis-à-vis de la sécurité des informations font partie des principales menaces envers les systèmes d'information. Une amélioration durable et significative de la sécurité des informations ne pourra pas être obtenue en mettant en place encore plus de solutions techniques et de processus sophistiqués. C'est en augmentant le niveau global de la sensibilisation à la sécurité et en éduquant tous les utilisateurs aux bases de la sécurité des informations* ». Et selon Eveloff, (2005), l'éducation et la sensibilisation correspondent à la plus importante des mesures à prendre en matière de sécurité des SI.

D'après (Pham et al, 2017), les utilisateurs finaux veulent être des participants autonomes, compétents, motivés et actifs dans le développement d'environnements sécurisés. Cependant, les gestionnaires veulent limiter l'autonomie pour s'assurer que les procédures sont suivies de près, plutôt que de permettre la flexibilité. Il en résulte la création d'environnements qui sont intrinsèquement démotivants plutôt que de motiver les utilisateurs finaux à devenir des cocréateurs autodéterminés et autorégulés d'un environnement informatique sécurisé. Dans ce sens, nous avons privilégié avoir l'avis des participants à la formation, pour savoir leurs préférences concernant le format de la formation, la durée, le contenu etc. Il s'avère que la plupart des participants souhaitent une formation simple, courte, des cas concrets, comment se protéger ? , des exemples de risques etc. Donc nous avons pris en considération les préférences des participants lors de la préparation du contenu de la formation. Dans la suite de cette étape, nous avons repris contact avec le dirigeant pour voir les disponibilités des équipes pour pouvoir intervenir au sein de la PME. Et pour la validation de la charte sécurité destinée aux utilisateurs du SI (Annexe 1), nous gardons l'anonymat de l'entreprise étudiée suite à la demande du dirigeant. Par contre, il nous paraît intéressant de présenter les caractéristiques de cette PME :

Taille	20 salariés
Secteur d'activité	Fabrication d'instrumentation scientifique et technique
Activité	L'instrumentation et l'analyse des eaux
Forme juridique	SARL
Chiffre d'affaire	7 009 K €

Tableau 1 : Caractéristiques de la PME étudiée

Avant d'accéder à notre terrain, nous avons préparé notre support de formation et les affiches et brochures de sensibilisation destinés aux participants. Ces supports ont été établis sur la base de la littérature sur la sécurité des SI, ainsi que les actualités et nouveautés dans le domaine de la sécurité des SI.

Etape 2 : Evaluation pré-intervention

Afin de pouvoir mesurer et évaluer l'effet de notre intervention dans l'amélioration de la sensibilité des utilisateurs du SI et dans la conduite du changement souhaité, nous avons préparé un questionnaire « Avant-intervention » qui prend son origine de la littérature.

Nous avons combiné deux échelles de mesure, nous avons adapté le questionnaire des aspects humains de la sécurité de l'information (HAIS-Q) de Parsons et al (2014) qui mesure la sensibilisation du répondant à la sécurité des SI, et qui est composé de 63 items qui évaluent sept domaines d'intervention, à savoir, gestion des mots de passe, utilisation d'e-mail, utilisation d'Internet, utilisation des réseaux sociaux, appareils mobiles, traitement de l'information et rapport d'incident. Chaque zone de mise au point est encore divisée en trois sous-domaines spécifiques, résultant en 21 domaines d'intérêt, dont chacun est mesuré par une connaissance, une attitude et un élément de comportement. McCormac et al (2017) affirment que quand nous développons des programmes de sensibilisation et de formation, le HAIS-Q pourrait être administré aux employés avant et après l'introduction du programme pour évaluer son efficacité. Ce qui justifie notre choix d'adopter ce questionnaire pour évaluer l'effet de notre intervention.

Pour compléter notre enquête, nous avons utilisé l'Information Security Culture Assessment (ISCA) qui est un instrument de mesure de la culture sécurité de l'information développé par Da Veiga & Martins (2015). L'ISCA comprend 45 déclarations réparties sur neuf construits

(Engagement, Importance, Efficacité des politiques, Directives de sécurité, Responsabilité, Nécessité, Actifs de sécurité, Surveillance, Conséquences).

Une échelle de Likert a été utilisée pour mesurer le degré d'accord ou de désaccord du répondant avec chaque affirmation. Le tableau suivant présente les principaux thèmes de notre questionnaire avec des exemples d'items proposés et leur origine.

Thème	Exemple d'items	Mesure culture	Mesure comportement	Origine
Gestion des mots de passe	- Un mélange de lettres, de chiffres et de symboles est nécessaire pour les mots de passe professionnels (Connaissance) -C'est sans danger d'avoir un mot de passe avec juste des lettres (Attitude) - J'utilise une combinaison de lettres, de chiffres et de symboles dans mes mots de passe professionnels (Comportement)	x	x	HAIS-Q
Utilisation des emails	Il est toujours sans danger de cliquer sur des liens dans les e-mails de personnes que je connais	x	x	HAIS-Q
Utilisation d'internet	Je vérifie la sécurité du site Web avant de saisir des informations	x	x	HAIS-Q
Utilisation des réseaux sociaux	Je peux publier ce que je veux concernant mon travail sur les réseaux sociaux	x	x	HAIS-Q
Ordinateur et WIFI	Il est risqué d'accéder à des fichiers de travail sensibles sur un ordinateur si quelqu'un peut voir mon écran	x	x	HAIS-Q
Traitement des informations	Je ne brancherai pas une clé USB trouvée dans un lieu public sur mon ordinateur de travail	x	x	HAIS-Q
Rapports d'incidents	Si j'ignore quelqu'un qui agit de manière suspecte sur mon lieu de travail, rien de mal ne peut arriver	x	x	HAIS-Q
Propriété de sécurité	Je sais quelles sont mes responsabilités en matière de sécurité de l'information	x		ISCA
Conformité à la sécurité	J'ai participé à une formation où j'ai eu des cours liés à la sécurité des systèmes d'information	x		ISCA
9	40 (Total des items)			

Tableau 2 : Thème du questionnaire et échelles de mesure utilisées

Le questionnaire « Avant intervention » a été transmis vers mi-octobre aux participants, qui représentent les utilisateurs des SI de l'entreprise (Annexe 2). Et en quelques jours, nous avons reçu les réponses de 11 participants.

Etape 3 : Sensibilisation et formation des utilisateurs

Dans cette étape, nous sommes intervenus deux jours au sein de la PME pour former et sensibiliser les participants qui sont divisés en deux groupes, le premier est formé de 6 personnes et le deuxième de 5 personnes. Notre intervention comprend deux volets : une formation et une sensibilisation à la sécurité. La formation s'est déroulée comme indiqué dans le tableau suivant :

Format	Exemples	Durée
Initiation à la sécurité	-Qu'est-ce que la sécurité -Comment peut-on définir le niveau de sécurité -Types et exemples d'attaques -Comment se protéger	15 min
Propositions des situations et échanges	-Protection des données -Politiques des mots de passe -Sécurité physique	20 min
Quizz (Kahoot)	-10 questions avec choix multiples -Classification des répondants selon leurs scores	15 min
Total		50 min

Tableau 3 : Le déroulement de la formation à la sécurité des SI

Lors de cette formation, nous avons fait recours à des méthodes ludiques et attractives (Propositions des scénarios et demander l'avis des participants, des Quizz) afin d'impliquer les participants et les rendre plus actifs avec la formation, en plus, le Quizz à la fin de la formation permet de voir leur classement par rapport à leurs collègues, et surtout sans jugement (ni sanctions, ni récompenses). La figure suivante montre un extrait de la classification des répondants :

Figure 3 : Classification des répondants aux questions du Quizz sur la sécurité des SI

Le deuxième volet de cette intervention, c'est la sensibilisation à la sécurité des SI à travers une brochure (Annexe3) distribuée aux participants, incluant des messages simples et positifs tels que : « *Sécurité des SI, je m'engage !* », « *Je veille à la confidentialité des données que je manipule* », « *Apportons tous notre contribution pour une meilleure sécurité* ». Ensuite une affiche de sensibilisation aux sauvegardes de données avec un message simple et positif (Annexe 4) a été confiée à la personne responsable des sauvegardes, pour qu'elle assure l'affichage dans les lieux les plus fréquentés par les salariés (Accueil, cafète, salle de réunion). Nous avons choisi de sensibiliser les utilisateurs à la sauvegarde de données, suite à une identification de faiblesses concernant les sauvegardes (fréquence de sauvegarde ; une fois par semaine, perte de données et blocage du système deux fois pour une durée qui dépasse une semaine). Notre objectif ici, est de sensibiliser les gens à une meilleure sauvegarde de données.

Etape 4 : Evaluation post-intervention

Cette étape consiste à évaluer l'effet de notre intervention sur le niveau de sécurité au sein de la PME concernée et plus précisément sur le niveau de sensibilité des participants et leurs comportements liés à la sécurité des SI.

Pour évaluer l'effet de l'intervention, nous avons distribué un questionnaire « Après-intervention » qui est déduit du questionnaire précédant « Avant-intervention », mais nous avons éliminé les questions où les répondants ont déjà un bon niveau (les meilleurs scores), donc nous estimons qu'il n'y aura pas une amélioration possible. Et ensuite nous avons rajouté

d’autres questions pour évaluer l’efficacité de l’intervention ainsi que le degré de satisfaction des participants. Le questionnaire après intervention est en annexe 5.

Selon Kotter (2006) le changement prend un temps considérable, surtout lorsqu'on vise à l'ancrer dans la culture d'une organisation, et pour Da Veiga et Eloff (2010), la culture de la sécurité de l'information change au fil du temps. Dans ce sens, le questionnaire « Après-intervention » a été distribué aux participants trois mois après notre intervention. Nous estimons que cette durée est acceptable pour commencer à observer les changements ou l’émergence d’une culture.

Après la réception de toutes les réponses, nous avons procédé à une comparaison entre les deux questionnaires « Avant et Après intervention » afin d’identifier les effets et les changements, de la culture sécurité ainsi que les comportements. À l'issue, de nos résultats qui seront présentés dans le titre suivant, nous avons fait un retour à la direction de cette PME, sur la situation établie : les points améliorés, les points qui restent à améliorer, des recommandations etc.

2. Les résultats de notre intervention

Nous allons représenter les résultats des deux questionnaires avant et après intervention dans le tableau suivant. En comparant les réponses des deux questionnaires, nous avons choisi de présenter les questions où nous avons remarqué une amélioration significative. Nous avons au total 11 réponses pour chaque questionnaire, dont 8 hommes et 3 femmes, leurs tranches d’âge varient entre :

- 18-24 ans : 3 répondants
- 25-34 ans : 5 répondants
- 35-44 ans : 1 répondant
- 45-54 ans : 2 répondants

Nous avons, 5 répondants qui occupent des postes liés à des informations sensibles (RH, comptabilité etc.) et 6 répondants dans des potes non liés à des informations sensibles.

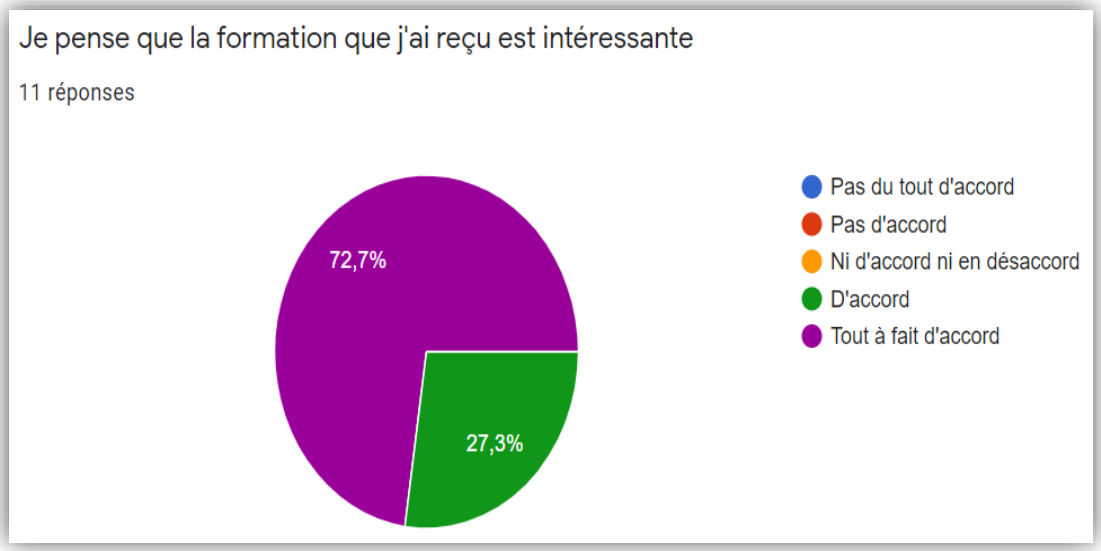
Item	Réponses avant intervention	Réponses après intervention
Je sais ce qu'est un incident de sécurité	D'accord : 7/11 Pas d'accord : 4/11	D'accord : 11/11 (100%)
Je suis autorisé à partager mon mot de passe avec des collègues	Pas du tout d'accord : 4 Pas d'accord : 3 Je ne sais pas : 3 D'accord : 1	Pas du tout d'accord : 5 Pas d'accord : 6
C'est une mauvaise idée de partager mes mots de passe professionnels, même si un collègue le demande	Pas d'accord : 3 Je ne sais pas : 3 D'accord : 1 Tout à fait d'accord : 4	Je ne sais pas : 1 D'accord : 6 Tout à fait d'accord : 4
Je partage mon mot de passe avec mes collègues	Pas d'accord : 9 D'accord : 2	Pas du tout d'accord : 6 Pas d'accord : 5
C'est sans danger d'avoir un mot de passe avec juste des lettres	Pas du tout d'accord : 4 Je ne sais pas : 3 D'accord : 3 Tout à fait d'accord : 1	Pas du tout d'accord : 9 Pas d'accord : 1 D'accord : 1
J'utilise une combinaison de lettres, de chiffres et de symboles dans mes mots de passe professionnels	Pas du tout d'accord : 1 Pas d'accord : 1 D'accord : 4 Tout à fait d'accord : 5	D'accord : 6 Tout à fait d'accord : 5
Je vérifie la sécurité du site Web avant de saisir des informations	Pas d'accord : 2 D'accord : 1 Tout à fait d'accord : 8	D'accord : 5 Tout à fait d'accord : 6
Je suis autorisé à entrer des informations sur n'importe quel site Web si cela m'aide à faire mon travail	D'accord : 2 Je ne sais pas : 3 Pas d'accord : 3 Pas du tout d'accord : 3	Je ne sais pas : 2 Pas d'accord : 4 Pas du tout d'accord : 5
Je sais quelles sont mes responsabilités en matière de sécurité de l'information	Pas du tout d'accord : 1 Pas d'accord : 1 Je ne sais pas : 5 D'accord : 2 Tout à fait d'accord : 2	D'accord : 5 Tout à fait d'accord : 6
Je connais les aspects de sécurité des informations liées à ma fonction professionnelle (par exemple, comment choisir un mot de passe ou gérer des informations confidentielles)	Pas du tout d'accord : 1 Pas d'accord : 1 Je ne sais pas : 3 D'accord : 4 Tout à fait d'accord : 2	D'accord : 5 Tout à fait d'accord : 6
Je crois que les exigences de sécurité des systèmes d'information devraient être intégrées à mes tâches quotidiennes.	Je ne sais pas : 8 Tout à fait d'accord : 3	Je ne sais pas : 3 D'accord : 4 Tout à fait d'accord : 4
Mes collègues font preuve d'engagement envers la SSI	Pas d'accord : 2 Je ne sais pas : 5 D'accord : 3 Tout à fait d'accord : 1	Je ne sais pas : 2 D'accord : 6 Tout à fait d'accord : 3

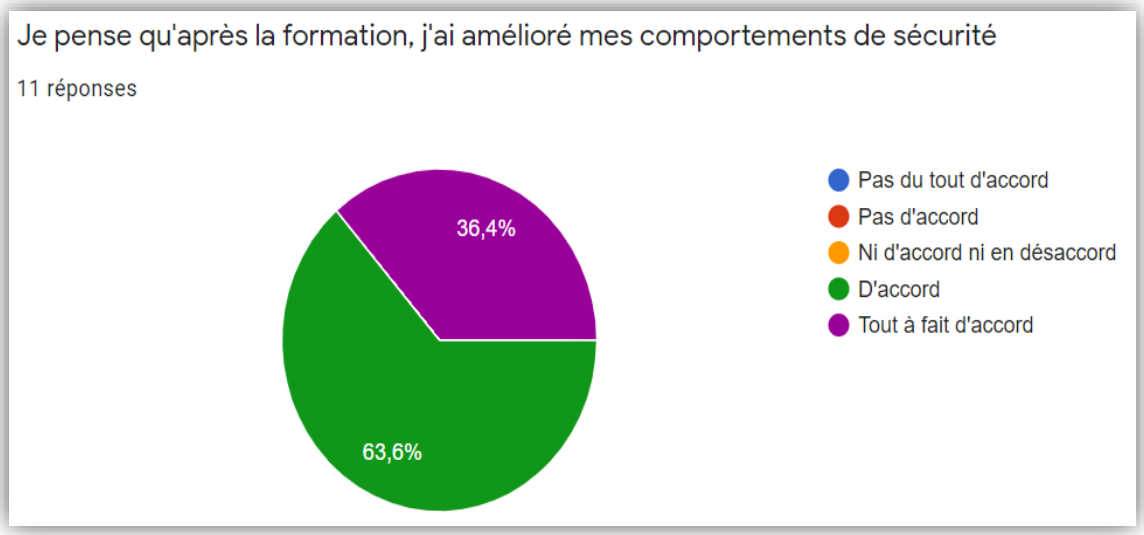
Tableau 4 : Comparaison entre réponses avant et après intervention

Suite à la comparaison des réponses avant notre intervention et les réponses après cette intervention, nous remarquons une amélioration significative au niveau de plusieurs items. Nous trouvons des items qui concernent la culture sécurité, à titre d'exemple : « Je sais ce qu'est un incident de sécurité », le pourcentage de réponses à cet item est passé de 63% de personnes « D'accord » à 100%. Un autre exemple, l'item « C'est sans danger d'avoir un mot de passe avec juste des lettres » qui mesure l'attitude de l'individu envers la gestion des mots de passe, le pourcentage de réponse de cet item passe de 36% de personnes qui sont « Pas du tout d'accord » à 81%.

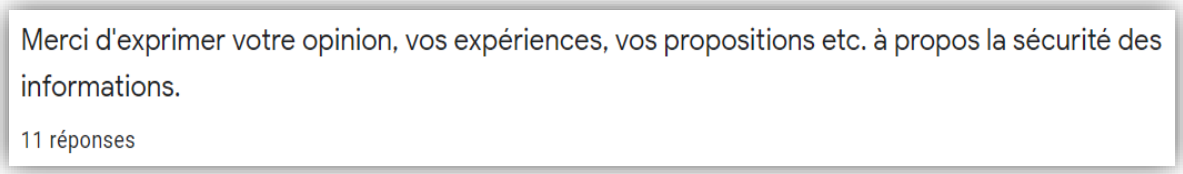
Ensuite, nous avons des items qui mesurent le comportement des répondants vis-à-vis des thèmes de sécurité, par exemple, l'item « Je partage mon mot de passe avec mes collègues » avec 18% des répondants qui partagent leurs mots de passe avec des collègues à aucun répondant qui partage ses mots de passe avec ses collègues après l'intervention. Un deuxième exemple d'item, « J'utilise une combinaison de lettres, de chiffres et de symboles dans mes mots de passe professionnels » avec un pourcentage de 18% qui ne le font pas avant l'intervention à 0% après l'intervention.

À la fin du questionnaire de l'après intervention, nous avons rajouté des questions afin de connaître l'avis des participants à propos la formation et la sensibilisation réalisée, ci-joint quelques exemples de questions posés et les résultats sous forme de graphiques (Google forms) :

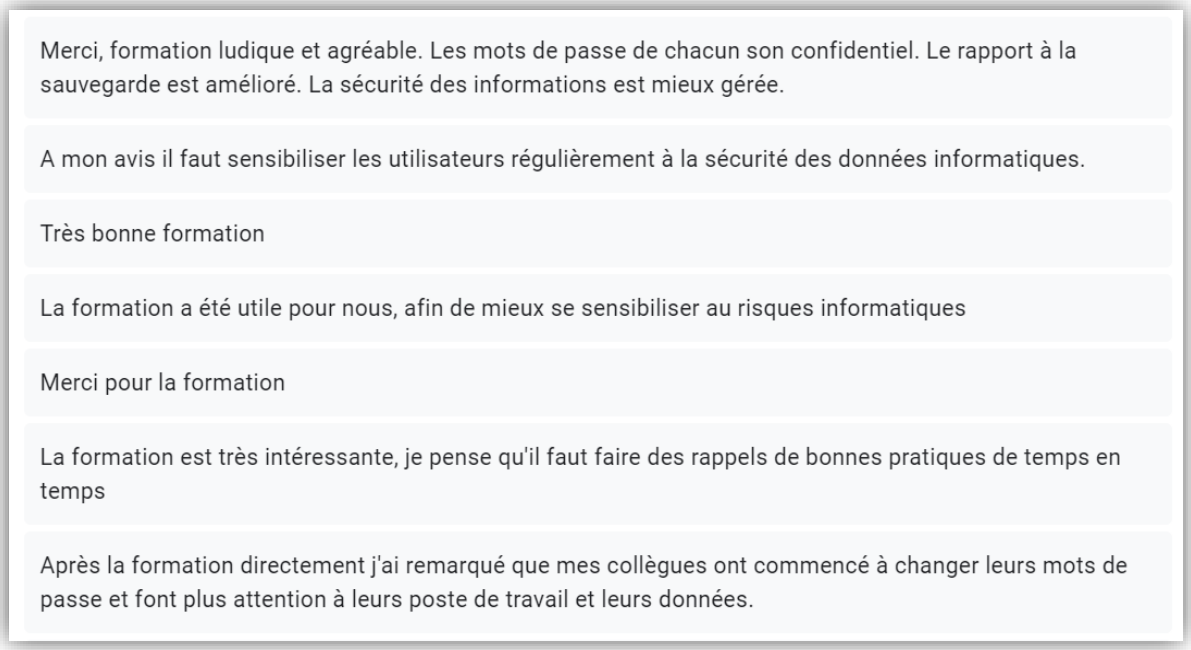




Nous avons posé une question ouverte à la fin du questionnaire qui est la suivante :

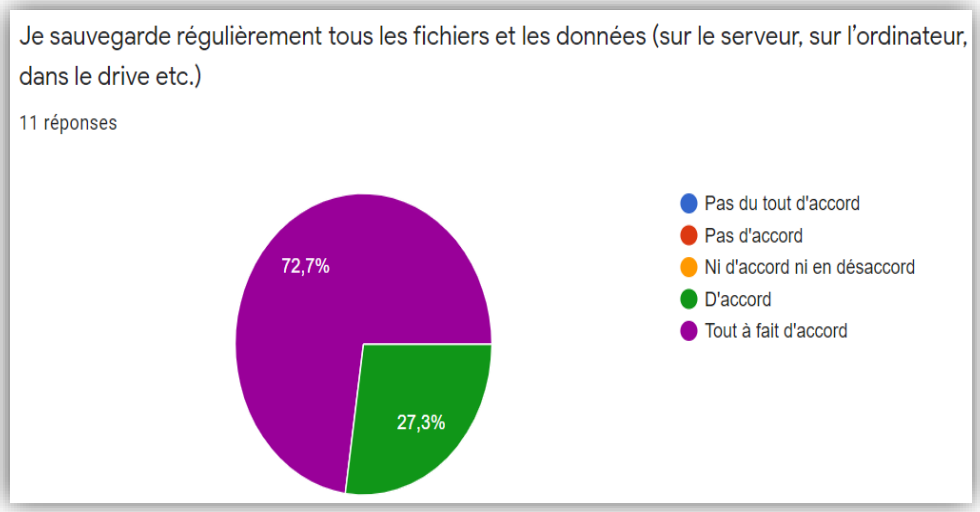


Voilà parmi les réponses reçues pour cette question :



Après les résultats issus de la comparaison les deux questionnaires, nous avons recontacté la personne responsable de la sauvegarde de données et à qui nous avons confié l'exposition de l'affiche de sensibilisation au sein de la PME pour avoir son retour et savoir s'il y a une

amélioration au niveau des sauvegardes. Cette personne travaille en bureau de conception, et son poste n'est pas en lien avec l'informatique, néanmoins, elle prend en charge la responsabilité de la sauvegarde de données. Cette personne a remarqué que les sauvegardes sont devenues plus rapprochées dans le temps et que ses collègues font plus attention aux données. En plus, le dirigeant de la PME a pris la décision de mettre en place un système de sauvegarde automatique sur le Cloud pour s'assurer que tout est bien sauvegardé à côté des sauvegardes manuelles faites par les utilisateurs. Le graphique suivant montre les réponses des répondants après l'intervention sur la question de sauvegarde des données :



Après l'exposition des résultats récoltés, nous allons dans le titre suivant, analyser ces résultats et les perspectives de notre recherche.

3. Discussion des résultats de l'intervention et affinage de la problématique

Suite à la comparaison entre l'évaluation pré-intervention et l'évaluation post-intervention de la culture sécurité et les comportements liés à la sécurité des participants, nous constatons qu'il y a une amélioration au niveau de la culture sécurité ainsi qu'au niveau des comportements liés à la sécurité. Cette amélioration se traduit par un sentiment de responsabilité plus élevé envers la sécurité des SI de l'entreprise, par des attitudes positives envers la gestion des mots de passe, l'utilisation des emails, d'Internet, des réseaux sociaux, et par une augmentation des comportements liés à la sécurité tels que l'utilisation des mots de passe plus robustes, le non partage des mots de passe avec les collègues ou la vérification de la sécurité du site web avant la saisie des informations.

Plusieurs travaux ont déjà montré l'efficacité de la formation et de la sensibilisation dans l'amélioration de la culture et les comportements liés à la sécurité, donc nous considérons que les résultats de notre intervention sont en cohérence avec ces travaux, parmi lesquels nous citons l'étude de Chen et al (2015) où les résultats montrent que la sensibilisation aux programmes SETA (Education, formation et sensibilisation) a une influence significative sur la culture de sécurité et sur les connaissances des employés.

Une formation à la sécurité peut contribuer à la création d'une culture sécurité en améliorant le comportement des employés et en augmentant leur niveau de sensibilisation à la sécurité. (Alnatheer et al, 2012), et une sensibilisation à la sécurité forme un pilier pour la mise en place d'une culture sécurité. (Hassan et Ismail, 2012 ; Da Veiga et Martins, 2015 ; Tolah et Al, 2017). Selon Barlette (2005), une sensibilisation (information et éducation) et/ou une formation pourraient être lancées afin de limiter les failles identifiées (faiblesse des mots de passe, manque de sauvegarde, fuite des données etc.). Une telle intervention pourrait s'avérer courte et donc peu coûteuse car ce sont surtout des principes basiques qu'il faudrait transmettre aux salariés. Et Da Veiga et Eloff, (2007), affirment que les organisations doivent veiller à ce qu' « *une culture de la sécurité de l'information soit inculquée par la formation, l'éducation et la sensibilisation, afin de minimiser les risques pour les actifs d'information* ».

Donc, selon les résultats de notre intervention, les actions de sensibilisation et de formation forment les prémisses d'une mise en place d'une culture de sécurité des systèmes d'information et des comportements liés à la sécurité, ceci est en cohérence avec la littérature.

Toutefois, lors de notre intervention, nous avons constaté l'existence d'autres facteurs qui peuvent influencer la création d'une culture et des comportements liés à la sécurité, tels que l'implication du dirigeant. Nous avons constaté une implication importante du dirigeant de cette PME à la sécurité des SI, à travers son engagement et sa réactivité. Tout au long du processus d'intervention, il a mis à notre disposition le matériel nécessaire pour réaliser notre intervention, il a assuré la diffusion du questionnaire auprès des participants et nous avons remarqué son soutien et son écoute vis-à-vis de ses collaborateurs. Il a exprimé son besoin d'un accompagnement pour améliorer la sécurité de son SI, et qu'il est prêt à mettre en place des procédures si cela permettra d'assurer cette amélioration. Ce constat, les travaux sur le TMS ou Top Management Support (Barlette, 2012 ; Boonstra, 2013) ont montré que le dirigeant a une influence majeure sur la validation de certains projets, sur les budgets affectés à ceux-ci, sur la

communication auprès des employés, voire sur les comportements des collaborateurs, surtout dans le cas des PME où le dirigeant joue un rôle central dans le choix et la mise en place des mesures et des contrôles liés à la sécurité des SI.

Cela nous mène à aller plus loin au niveau de la littérature afin de déterminer les facteurs qui peuvent jouer sur l'émergence et l'amélioration de la culture et des comportements liés à la sécurité et afin d'étudier la culture sécurité dans son ensemble, et d'une vision plus systémique. De plus, la sécurité des systèmes d'information met en jeu des problématiques organisationnelles qui sont de nature complexe (Morin, 1990; Genelot, 1998), et des problématiques humaines qui sont liées à une « hypercomplexité » (Morin, 1990), ce qui peut justifier, notre intention d'aller plus loin dans la recherche des facteurs en lien avec la mise en place d'une culture sécurité des SI.

Au niveau de la littérature, nous trouvons des auteurs qui parlent des facteurs qui influencent la culture sécurité (Hassan et Ismail, 2012), l'existence des facteurs externes et des facteurs internes (Djokovski et al, 2007) et d'autres auteurs qui évoquent des facteurs qui influencent la culture sécurité et des facteurs qui la constituent (Alnatheer et al, 2012 ; Alnatheer, 2014 ; Tolah et al 2017). Nous avons identifié plusieurs cadres et modèles au niveau de la littérature, qui tentent la compréhension et l'évaluation de la culture sécurité. Nous allons développer et analyser ces cadres au niveau de la première partie de notre travail, afin de mettre en lumière ce qui peut influencer et déterminer la culture sécurité des SI, et plus particulièrement dans le cadre des PME. Le schéma suivant récapitule le cheminement suivi pour délimiter notre objet de la recherche à partir de l'interaction entre la littérature et l'intervention réalisée.

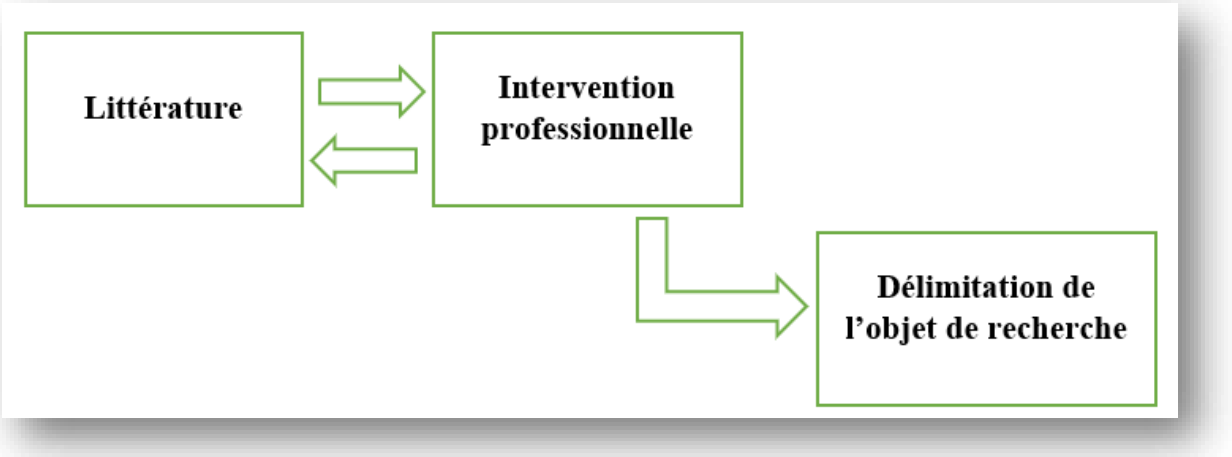


Figure 4 : Délimitation de l'objet de recherche

Conclusion du chapitre préliminaire

Ce chapitre préliminaire décrit les étapes mises en place lors de notre intervention au sein d'une PME. Cette intervention se traduit par une sensibilisation et une formation destinées à un groupe d'utilisateurs des systèmes d'information d'une PME dans l'objectif d'améliorer la culture sécurité et les comportements liés à la sécurité des SI de ses utilisateurs. L'évaluation pré-intervention et l'évaluation post-intervention ont permis de démontrer l'efficacité de la mise en place d'une sensibilisation et une formation dans l'amélioration de la culture et des comportements des utilisateurs dans la sécurité des SI de l'entreprise.

Dans une optique d'exploration et avec un aller-retour entre théorique et pratique, nous avons identifié que l'amélioration et la création d'une culture sécurité ne se limite pas uniquement à une sensibilisation et/ou une formation mais dépend aussi d'autres facteurs que nous allons étudier en profondeur lors de nos parties suivantes.

Donc la question de la mise en place d'une culture sécurité des systèmes d'information doit être prise en compte dans sa globalité et analysée dans une logique plus systémique en prenant en compte tous les facteurs qui peuvent jouer un rôle dans la création ou l'amélioration de la culture sécurité.

Partie I
Conception d'une culture sécurité des SI en PME : vers un modèle conceptuel

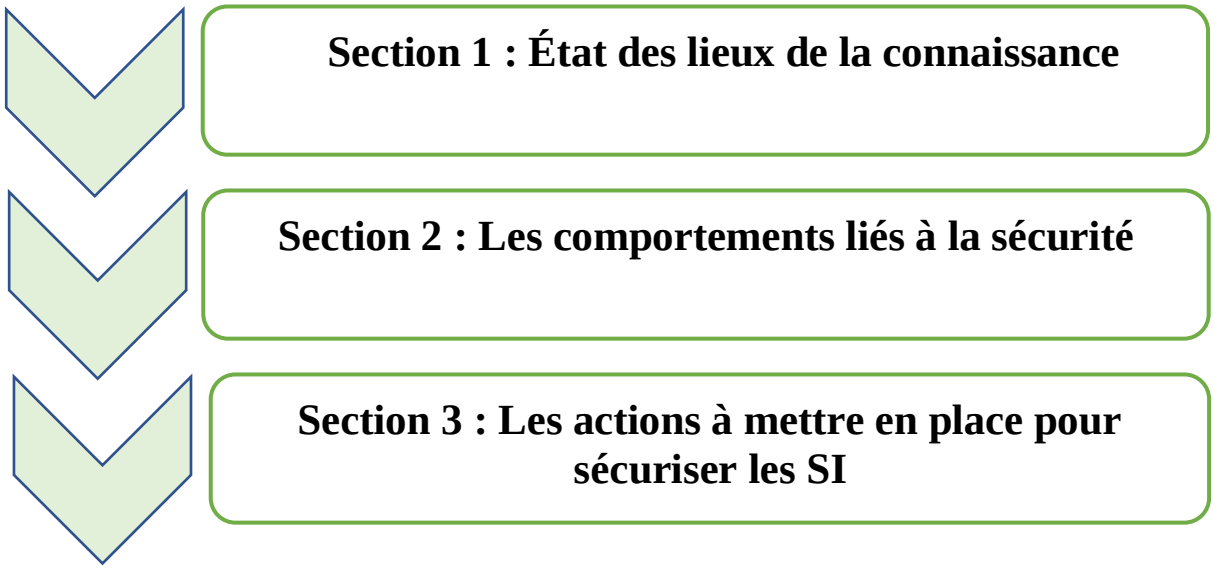
Nous nous attachons dans cette première partie à présenter les fondements théoriques dans le domaine de la sécurité des systèmes d'information et plus particulièrement au sein des PME. Dans cette optique, nous nous penchons dans un premier temps sur une revue de littérature sur la culture sécurité des systèmes d'information dans les PME **(chapitre 1)**. Ensuite, nous proposons un modèle théorique de la culture sécurité des systèmes d'information adapté au contexte de la PME avec des orientations de recherche qui permettent la compréhension des relations entre les construits de ce modèle **(chapitre 2**).

Chapitre 1
La culture sécurité des systèmes d'information dans les PME

Afin de comprendre la culture sécurité des membres des organisations et plus particulièrement des PME face aux systèmes d'information, nous allons présenter les définitions des chercheurs qui ont tenté de définir le concept de la culture sécurité des systèmes d'information. Ensuite, nous allons présenter une revue de littérature sur la culture sécurité avec les théories et les modèles qui nous ont marqué le plus dans ce domaine. À la fin de la section, nous analysons la relation entre la culture sécurité et la culture organisationnelle **(Section 1)**

Ensuite, nous examinons les comportements liés à la sécurité à travers un état d'art des théories et modèles dans le domaine des comportements. Et en fin de la section, nous discuterons la relation entre la culture sécurité et les comportements liés à la sécurité. **(Section 2)**

Nous conclurons ce chapitre par la présentation des mesures de sécurité qu'une organisation, plus particulièrement une PME peut mettre en place afin de garantir un niveau acceptable de sécurité de ses systèmes d'information. **(Section 3)**



Section 1 : État des lieux de la connaissance

Cette section est consacrée à l'examination de la culture sécurité en commençant par une revue de littérature dans ce domaine, en passant par la gestion du changement de la culture sécurité et les instruments de mesure de la culture sécurité et en finissant par la culture sécurité dans le cadre des PME.

1. La culture sécurité des systèmes d'information:

1.1 Vers une définition de la culture sécurité des systèmes d'information

Après la réalisation de notre revue de littérature, nous avons essayé de répondre à la question suivante : Qu'entend-on par culture sécurité des systèmes d'information ?

1.1.1 Notions : Culture, sécurité

Penchons-nous d'abord sur le terme « Culture ». C'est à l'anthropologie anglaise que revient ce concept, plus exactement à E.B. Tylor dans *Primitive Culture* parut en 1871, s'inspirant en particulier des travaux de Gustav Klemm pour tirer les éléments dont il avait besoin pour former la notion de culture, qu'il employa comme synonyme de civilisation. Dans son ouvrage, Tylor (1871) donna une définition de la culture comme : « *La culture ou la civilisation, entendue dans son sens ethnographique étendu, est cet ensemble complexe qui comprend les connaissances, les croyances, l'art, le droit, la morale, les coutumes, et toutes les autres aptitudes et habitudes qu'acquiert l'homme en tant que membre d'une société* ». Cette définition, se rapporte à un ensemble de faits qui peuvent être directement observés en un moment donné du temps (Guy Rocher, 1992). En sociologie, le terme culture a été adopté par les premiers sociologues américains, en particulier Albion Small, Park, Burgess et Ogburn. Il fut cependant plus lent à s'y frayer un chemin qu'en anthropologie, vraisemblablement parce que les grands précurseurs de la sociologie, Comte, Marx, Weber, Durkheim ne l'ont pas employé, mais il fait partie du vocabulaire de la sociologie aussi bien que de l'anthropologie (Guy Rocher, 1992).

En s'inspirant de la définition de Tylor et de plusieurs autres (Kroeber et Kluckhohn, 1952), le sociologue québécois Guy Rocher donne une définition à la culture : « *un ensemble lié de manières de penser, de sentir et d'agir plus ou moins formalisées qui, étant apprises et*

partagées par une pluralité de personnes, servent, d'une manière à la fois objective et symbolique, à constituer ces personnes en une collectivité particulière et distincte » (Guy Rocher, 1969). Prenons la définition de l'institution internationale UNESCO[7] (1982) : « *La culture peut aujourd'hui être considérée comme l'ensemble des traits distinctifs, spirituels, matériels, intellectuels et affectifs, qui caractérisent une société ou un groupe social. Elle englobe, outre les arts, les lettres et les sciences, les modes de vie, les lois, les systèmes de valeurs, les traditions et les croyances* ».

Pour G. Hofstede (1987) : « *La culture est par essence une organisation mentale collective ; cette partie de notre conditionnement que nous partageons avec les autres membres de notre nation, de notre région, de notre groupe, mais aussi avec ceux d'autres nations, d'autres régions ou d'autres groupes* ».

Toutes ces définitions abordent la notion du **collectif**. Le nombre de personnes importe peu, il peut suffire de quelques personnes pour créer la culture d'un groupe restreint, alors que la culture d'une société globale est nécessairement partagée par un plus grand nombre de personnes. Les façons d'être doivent être considérées comme idéales ou normales par un nombre suffisant de personnes pour qu'on puisse reconnaître qu'il s'agit bien de règles de vie ayant acquis un caractère collectif et donc social. (Guy Rocher, 1992).

Quant à elle la notion de « Sécurité » vient du mot latin « *securitas* » signifiant exemption de soucis, tranquillité d'esprit. Elle est omniprésente dans les préoccupations quotidiennes des individus. Elle touche pratiquement tous les aspects de la vie. On parle de la sécurité de l'individu, de la sécurité sociale, de la sécurité nationale, de la sécurité aérienne, de la sécurité routière, de la sécurité alimentaire, etc. (Ayse Ceyhan, 1998).

Dans sa contribution au *Critical Security Studies*, Simon Dalby (1997) reprend la formule employée par Buzan (1993) pour caractériser le concept de sécurité comme un « *essentially contested concept* » qui désigne en français « concept essentiellement contesté ». Cette expression signifie que le concept de sécurité est l'objet de contestations et qu'il revêt plusieurs significations qui ne sont pas nécessairement liées à la définition conventionnelle. Un concept essentiellement contestable est un concept qui n'existerait pas en tant que concept sans les usages concurrents dont il est l'objet (Dario Battistella 2009).

[7] UNESCO : Déclaration de Mexico sur les politiques culturelles. Conférence mondiale sur les politiques culturelles, Mexico City, 26 juillet - 6 août 1982.

Pour certains, analyser le sens de la sécurité revient à la définir c'est-à-dire lui donner une signification. Pour d'autres, comme Ole Waever (1997), il faut conceptualiser la sécurité en lui donnant un contenu spécifique plus large et plus complexe, communicable par le langage. Donc la définition centralise la recherche dans un registre particulier. Quant à elle, la conceptualisation explore plus en détail ce qui caractérise une politique de sécurité ainsi que le débat qu'elle engendre.

Sans entrer dans le débat définition ou conceptualisation, Dillon (1996) se propose d'examiner l'étymologie et la généalogie du terme. La généalogie s'interroge sur l'entrée de la sécurité dans le discours. L'étymologie attire l'attention sur l'ordre du discours et sur ses termes essentiels en rappelant leur sens véritable. Pour cet auteur, la sécurité est un terme dual qui signifie non seulement un moyen de libération à l'égard du danger, mais aussi un moyen de le limiter. Comme la sécurité est engendrée par la peur, elle nécessite des contre-mesures pour contrôler, contenir, neutraliser, éliminer cette peur. Ainsi, tout en nous apprenant de quoi il faut avoir peur, elle cherche aussi à proscrire, à sanctionner en quelque sorte à mettre en danger ce qui nous menace (Ceyhan, 1998).

Il a été avancé que la mesure de la sécurité et de la culture est un processus complexe qui prendra beaucoup de temps à enquêter et est extrêmement difficile à généraliser à une large population (Schlienger et Teufel, 2003). Par conséquent, le défi à relever est de quantifier et d'étudier les éléments critiques qui conceptualisent et mesurent la culture de sécurité.

Nous allons maintenant nous attarder sur la différence entre les concepts suivants : la sécurité de l'information, la sécurité informatique et la sécurité des systèmes d'information afin de limiter l'ambiguïté qui peut apparaître entre ces trois concepts.

1.1.2 Différenciation des concepts voisins : Sécurité de l'information, sécurité informatique et sécurité des systèmes d'informations

Avant de définir ce qu'est la culture de sécurité des systèmes d'information, nous allons faire une distinction entre ce qui est : sécurité de l'information, sécurité informatique et sécurité des systèmes d'information. Tout d'abord, nous allons présenter ce qu'est l'information.

Selon P. Romagni et V. Wild (1998), l'information est considérée comme « *un renseignement qui améliore notre connaissance sur un sujet quelconque* ». Cette définition positionne

l'information comme une source de connaissance. La question qui se pose ici est : pourquoi cherchons-nous à protéger cette information ?

L'information représente une "ressource économique, disponible dans les organisations, et comme toute ressource, elle a une valeur et un coût." (J.C. Emery, 1969). Et c'est cette valeur et ce coût qui rendent nécessaire sa protection.

Plusieurs organismes et auteurs ont proposé des définitions de la notion de **sécurité de l'information** comme (McDermott et Geer, 2001 ; Venter et Eloff, 2003 ; ISACA, 2008). Prenons comme exemples les définitions suivantes :

« *... La sécurité de l'information est une discipline de gestion des risques, dont le travail est de gérer le coût du risque de l'information pour l'entreprise* » Blakley et al, (2001).

« *La sécurité de l'information est la protection de l'information et minimise le risque d'exposer des informations à des tiers non autorisés* » (Venter et Eloff, 2003).

Ces deux définitions abordent la notion de gestion des risques. Pour ces auteurs, la notion de sécurité de l'information est étroitement liée à la notion de risque de l'information. La sécurité de l'information est donc la protection de l'information contre tous risques.

Avant de tenter de se protéger, il est nécessaire de déterminer quelles sont les informations sensibles de l'entreprise, qui peuvent être des données, ou plus généralement des actifs représentés par des données. Les actifs forment aussi et en particulier le capital intellectuel de chaque entreprise qui présente un patrimoine informationnel à protéger. Il faut donc évaluer les menaces et déterminer les vulnérabilités pour ces éléments sensibles à travers une gestion et une évaluation des risques. La sécurité peut s'évaluer à travers plusieurs critères :

-Disponibilité : propriété d'accessibilité au moment voulu des biens par les personnes autorisées,

-Intégrité : propriété d'exactitude et de complétude des biens et informations,

-Confidentialité : garantie que seules les personnes autorisées ont accès aux éléments reconnus.

Quant à lui, le **système informatique** va désigner les outils. Prenons la définition de Barlette (2006) adaptée de celle de Reix, (1984) : « *un ensemble d'éléments, matériels et logiciels permettant d'acquérir, traiter, mémoriser, communiquer des informations* ». Récemment, on

parlait de « sécurité informatique », appellation qui réfère la sécurité à des éléments technologiques : les systèmes de sauvegarde, l'antivirus ou les firewalls, sans mettre l'accent sur les aspects humains et organisationnels.

Le Moigne, (1973) précise qu'il ne faut pas confondre le système d'information et le système informatique. Il cite à son tour Deloche de Noyelle et Westercamp, (1971) : « *l'informatique n'est qu'une partie du système d'information; celui-ci englobe tout ce qui touche à l'information : les procédures manuelles, les circuits des informations, les dispositifs de saisie et de transmission des données, les méthodes d'obtention et de présentation des documents, etc. …* ».

Donc, la **sécurité informatique** est l'ensemble des règles, outils et procédures techniques mis en place pour préserver la confidentialité, l'intégrité et la disponibilité des données traitées par les systèmes informatiques.

Posons maintenant la question suivante : qu'entendons-nous par « **Systèmes d'information** » ?

Selon R.Reix et F.Rowe, (2002) « *Un système d'information est un ensemble d'acteurs sociaux qui mémorisent et transforment des représentations via des technologies de l'information et des modes opératoires* ». Cette définition présente l'aspect humain et l'aspect organisationnel qui s'ajoutent à l'aspect technique pour former tout un système complexe et complet de l'information.

Selon Archimbaud et Longeon (1999), le concept de sécurité des systèmes d'information recouvre un ensemble de méthodes, techniques et outils, chargés de protéger les ressources d'un système d'information afin d'assurer:

- **La disponibilité des services**: Les services (ordinateurs, réseaux, périphériques, applications…) et les informations (données, fichiers…) doivent être accessibles aux personnes autorisées quand elles en ont besoin;

- **La confidentialité des informations:** Les informations n'appartiennent pas à tout le monde; seuls peuvent y accéder ceux qui en ont le droit.

- **L'intégrité des systèmes:** Les services et les informations (fichiers, messages…) ne peuvent être modifiés que par les personnes autorisées (administrateurs, propriétaires…).

Pour résumer la différence entre ces trois notions, la **sécurité informatique** s'intéresse essentiellement à la composante technique du Système d'Information, alors que la **Sécurité du Système d'Information (SSI)** s'intéresse également aux composantes humaines et

informationnelles du Système d'Information. Et quant à elle, la **sécurité de l'information** « non numérique » sous forme de document papier, de savoir, etc. doit être également prise en compte par la sécurité du système d'information. Nous montrons à travers le schéma suivant une représentation de ces trois notions en fonction des considérations organisationnelles (humaines et informationnelles) et des considérations techniques prises en compte :

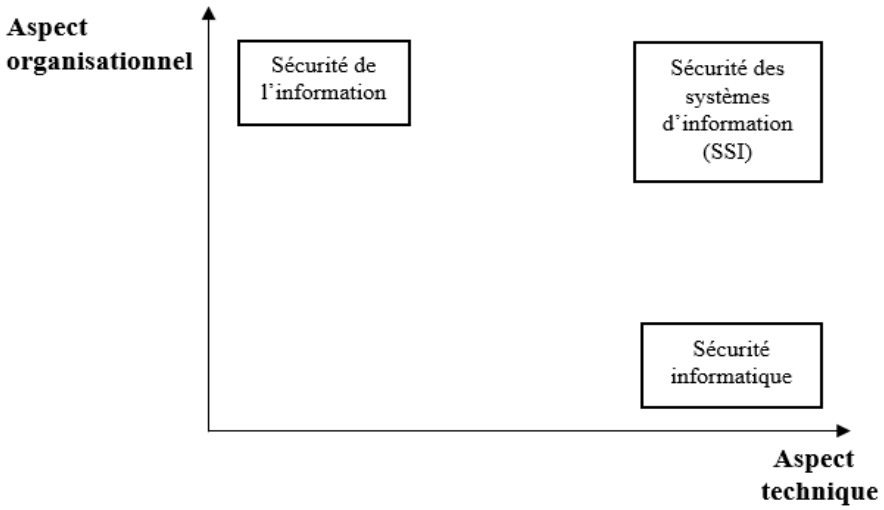


Figure 5 : Positionnement de la sécurité informatique, la sécurité de l'information et la SSI selon leurs aspects techniques et organisationnels

1.1.3 La culture sécurité de l'information

Plusieurs auteurs ont tenté de définir le concept de la culture sécurité de l'information (Dhillon, 1999 ; Von Solms 2000 ; Schlienger et Teufel, 2003 ; Da Veiga et Eloff, 2010 ; AlHogail et A. Mirza, 2014). Selon Schlienger et Teufel (2003) : « *La culture de la sécurité englobe toutes les mesures socioculturelles qui soutiennent les mesures de sécurité techniques, de sorte que la sécurité de l'information devient un aspect naturel dans les activités quotidiennes de chaque employé. Le concept culturel contribue à accroître la confiance entre les différents acteurs concernant la sécurité de l'information au sein d'une organisation ».*

Cette définition présente trois aspects, à savoir **l'aspect social**, **l'aspect culturel** et **l'aspect technique** où les mesures sociales et culturelles viennent soutenir les aspects techniques de la sécurité. Le résultat de l'interaction entre ces trois aspects est que la culture sécurité devient un **aspect naturel** dans les activités quotidiennes de chaque employé.

La définition la plus utilisée dans la littérature est celle proposée par Da Veiga et Eloff (2010) : « *La culture de la sécurité de l'information se compose des attitudes, hypothèses, croyances,*

valeurs et connaissances que les employés et les parties prenantes utilisent pour interagir avec les systèmes et les procédures de l'organisation à tout moment. L'interaction aboutit à un comportement acceptable ou inacceptable qui se manifeste dans les artefacts et les créations qui font partie intégrante de la façon dont les choses sont effectuées dans l'organisation pour protéger ses actifs informationnels ».

Ces deux auteurs ont basé leur définition sur la définition de la culture organisationnelle telle qu'elle est présentée par E. Shein (1985), où l'existence de trois niveaux, ou couches, permet d'identifier une culture au sein d'une organisation, à savoir les artefacts, les valeurs partagées et les hypothèses de base que nous détaillons dans la sous-section 2 de ce chapitre (Culture sécurité et culture organisationnelle).

La définition de Da Veiga et Eloff met en valeur l'interaction de la culture sécurité, les systèmes et les comportements des employés pour protéger les actifs informationnels. Cette définition aborde d'un côté, la relation entre culture sécurité et comportements lié à la sécurité et d'un autre côté, évoque l'interaction entre les utilisateurs et les systèmes et les procédures. Nous remarquons que cette définition peut définir à la fois la culture sécurité de l'information et la culture sécurité d'un système d'information puisque la sécurité de l'information fait partie de la sécurité du système d'information.

Malgré l'importance des définitions précédentes pour reconnaître la nécessité de créer une culture de la sécurité afin de gérer efficacement la sécurité, ces définitions se concentrent uniquement sur la manifestation d'une culture de la sécurité de l'information au sein des organisations. Ils définissent ce qu'est la culture de sécurité, ce qu'elle reflète. Ces définitions n'ont pas spécifiquement discuté des facteurs ou des concepts qui constituent ou conceptualisent la culture de la sécurité de l'information.

Certains chercheurs se concentrent uniquement sur le développement d'une compréhension des concepts de la culture de la sécurité de l'information (OECD[8], 2005; Tessem et Skaraas, 2005); ou fournissent un ensemble de principes (Kraemer et Carayon, 2005; Ruighaver et al. 2007). D'autres chercheurs ont effectué une étude pour illustrer une façon de cultiver la culture sécurité de l'information en développant un cadre (Dojkovski et al. 2006; Da Veiga et Eloff, 2010; Alnatheer et al. 2012; Alhogail et al. 2015; Sherif et al. 2015) ou en évaluant la culture de la sécurité de l'information (Martins et Eloff, 2002; Schlienger et Teufel, 2005; Da Veiga et Eloff,

[8] OECD : Organisation de coopération et de développement Economiques

2010). L'analyse de la littérature a montré que la plupart des études disponibles ont démontré qu'il existe divers facteurs importants qui pourraient façonner ou modifier la culture SSI (Alhogail et Mirza, 2014). Afin d'aller plus loin, nous allons présenter les différents facteurs qui influencent la culture sécurité ainsi que les facteurs qui constituent cette culture ultérieurement et plus particulièrement au niveau du chapitre 2.

Lors de notre revue de littérature sur la définition de la culture de la SSI, nous avons constaté deux types de définitions, celles classées selon une perspective « Employés » qui se rapportent principalement aux comportements ou à l'attitude des employés telles que les définitions de : Dhillon (1997), Martins & Eloff (2002), Helokunnas & Kuusisto (2003), Schlienger & Teufel (2003), Ngo et al. (2005), Ross (2011) Da Veiga & Eloff (2010), Da Veiga & Martins (2015), Astakhova (2014), et celles qui sont classées selon une perspective « Organisation », qui s'intéressent plutôt aux activités conduites par l'organisation en termes de sécurité de l'information telles que les définitions de : Von Solms (2000), Helokunnas & Kuusisto (2003), Vroom & Von Solms (2004), Ruighaver et al. (2006).

Pour mieux comprendre cette classification, quelques définitions sont présentées ici. La plupart des définitions de la culture de la sécurité de l'information s'inscrivent selon la perspective des employés. Astakhova (2014) stipule que la culture de la sécurité de l'information est la réception et l'envoi de modèles de valeurs relatifs à la sécurité de l'information entre un employé et l'organisation. Martins & Eloff (2002), Ngo et al. (2005) et Ross (2011) perçoivent la culture de la sécurité de l'information telle que la manière dont les choses sont faites au sein d'une organisation, c'est-à-dire les comportements acceptés vis-à-vis de la sécurité de l'information. Pour Helokunnas & Kuusisto (2003), la culture de la sécurité de l'information est un système de composantes qui comprend les attitudes des individus, leurs motivations, leurs connaissances et leurs modèles mentaux à l'égard de la SSI. Ces mêmes auteurs, Helokunnas & Kuusisto (2003), ont défini la culture de la sécurité de l'information d'une perspective organisationnelle. Pour eux, la culture de la sécurité de l'information est l'application d'un cadre qui contient des composantes telles que la standardisation, la certification, et la mesure de la sécurité de l'information. Pour Von Solms (2000), une culture de la sécurité de l'information est une culture organisationnelle qui soutient les politiques et les procédures de sécurité, les méthodes et les responsabilités de l'organisation afin que la sécurité de l'information devienne naturelle dans la réalisation des tâches des employés. La définition de Vroom et Von Solms (2004) soutient ce dernier point puisqu'il décrit la culture de la sécurité de l'information comme étant une culture utopique où les employés suivent les règles

organisationnelles comme si elles faisaient partie de leur seconde nature. Et enfin, pour Ruighaver et al. (2006) la culture de la sécurité de l'information reflète comment la direction d'une organisation gère la sécurité de l'information.

1.1.4 Culture sécurité des systèmes d'information : proposition de définition

L'analyse conduite sur la définition de la culture sécurité des systèmes d'information issue de la littérature montre que le construit souffre de l'absence d'une définition. En se basant sur les éléments qui définissent ce qu'est un système d'information, ce qu'est la culture et les définitions proposées dans la littérature sur la culture sécurité de l'information, nous allons proposer une définition de la culture sécurité des systèmes d'information qui est la suivante :

> « *La culture sécurité des systèmes d'information est l'ensemble des manifestations visibles et invisibles partagées par les membres d'une organisation. Ces manifestations incluent les hypothèses, les croyances, les valeurs, les artefacts et les pratiques formelles et informelles qui influencent les actions et les comportements des utilisateurs concernant la protection du système d'information de l'organisation* ».

Cette définition permet d'identifier les éléments qui pourraient s'avérer particulièrement importants pour expliquer la mise en œuvre de pratiques de sécurité par les utilisateurs d'un système d'information. Cette définition permet aussi de donner un éclairage différent quant à la relation entre les éléments de la culture et les comportements de sécurité qui sont influencés par ces éléments.

En ce qui concerne la définition de tout ce qui est valeurs, croyances, hypothèses et artefacts, elle sera bien détaillée et développée dans la suite de notre thèse et plus particulièrement, au niveau du deuxième chapitre de cette première partie.

Dans la suite de notre travail et au niveau de notre revue de littérature, nous nous intéressons à la culture sécurité de l'information, la culture sécurité informatique et à la culture sécurité des SI. Par souci de simplification, nous avons choisi de mobiliser le terme **sécurité des SI (SSI)** pour désigner la sécurité du SI, de l'information ou du système informatique, car le système d'information englobe l'informatique et les informations. Nous rappelons les propos de Deloche de Noyelle et Westercamp, (1971) : « *l'informatique n'est qu'une partie du système d'information; celui-ci englobe tout ce qui touche à l'information : les procédures manuelles,*

les circuits des informations, les dispositifs de saisie et de transmission des données, les méthodes d'obtention et de présentation des documents, etc. … ».

1.2 État de l'art des travaux sur la culture SSI : Théories et modèles

Karlson. F et al (2015) ont effectué une revue de littérature de la culture sécurité, des travaux réalisés entre 2000 et 2013, ils ont constaté que 25% des travaux traitent des questions relatives à la nature de la culture sécurité et 43% des travaux cherchent les racines de la culture sécurité. Ils concluent que le fait que la plupart de ces travaux se retrouvent dans ces catégories, indique que ce domaine de recherche en est à ses débuts. Ils ont trouvés que près du tiers des articles cherchent à savoir comment cultiver une culture de la sécurité des SI. Le tableau suivant présente les trois catégories de classification de ces travaux selon des méta-questions proposées par ces chercheurs. Nous avons rajouté les travaux effectués entre 2013 et 2021 à ces catégories.

Meta-question	Sujet de recherche	Références
Qu'est-ce que la culture sécurité des SI?	-Cadre pour comprendre la culture sécurité SI -Approches pour évaluer la culture sécurité SI - Analyse des cultures de sécurité existantes	-Alnatheer 2014, Harnesk et Lindström, 2011; Van Niekerk et Von Solms, 2010; Alfawaz et al. 2010, -Tolah et al. 2017, Okere et al. 2012; Ghernaouti-Hélie et al. 2010; Gaunt, 1998, - Kolkowska, 2011; Ramachandran et al. 2008.
Quelles sont les racines de la culture sécurité du SI?	-La relation entre la culture (organisationnelle) et la sécurité du SI - Facteurs contribuant à la culture sécurité du SI	- McCoy et al. 2009; Goo et al. 2013; Connolly et Lang, 2012, - Knapp et al. 2007; Alnatheer et Nelson, 2009, Shahibi et al. 2012;
Quels sont les fruits de différentes cultures sécurité SI?	-Identification de la culture sécurité dominante et ses sous-cultures	-Da Viega et Martins, 2017
Comment cultiver une culture sécurité du SI?	-Cadre pour cultiver une culture de la sécurité SI - Défis de management - Pratiques existantes - Travail pratique pour cultiver une culture sécurité SI	- Tolah et al. 2017, Sherif et Furnell 2015, Da Viega et Eloff, 2010; Thomson et al. 2006; Williams, 2008, Nemati et Church, 2009, - Ashenden, 2008; Ghernaouti-Hélie, 2009; Dojkovski et al. 2007a; Gaunt, 2000; Johnsen et al. 2006, -Von Solms, 2000, Lacey, 2010, - Johnson et Goetz, 2007; Ashenden et Sasse, 2013

Tableau 5 : Sujets de recherche enquêté sur la CSSI adapté de Karlson. F et al (2015)

Selon (Ngo, Zhou, et Warren, 2005) la CSSI est souvent expliquée à l'aide d'une variété de théories et de principes établis issus d'autres domaines de recherche. En effet, la CSSI est un domaine de recherche nouveau et émergent. Il est donc logique d'utiliser d'autres théories comme base de recherche. Parmi ces théories, nous remarquons la forte présence des théories liées à la culture organisationnelle. Nous allons présenter sa relation avec la culture sécurité dans le titre suivant (2). Karlson. F et al (2015) montrent que sept disciplines de référence ont contribué avec des théories à la recherche sur la CSSI, à savoir : l'anthropologie, l'économie, la gestion des connaissances, les sciences organisationnelles, la psychologie, la philosophie et la sociologie. Parmi ces disciplines, la plupart des théories ont été empruntées à la science organisationnelle et à la psychologie. Selon ces auteurs, il n'est pas surprenant que plusieurs de ces théories soient des modèles culturels / typologies de cultures (Schein, 1985; Hofstede, 1997; Westrum, 1993; Detert et al. 2000). Pour mettre en évidence les théories qui ont eu un impact sur plusieurs sujets de recherche, Karlson. F et al (2015) inclurent le modèle culturel de Schein (1985) et le cadre culturel national de Hofstede (1997); tous les deux proviennent de la science organisationnelle. Après l'inventaire des principaux sujets de recherche dans le domaine de la CSSI ainsi que les théories de différentes disciplines exploitées dans ce domaine, nous allons présenter dans les titres suivants les cadres et les théories pour comprendre la CSSI, les approches pour évaluer cette culture ainsi que les cadres proposés pour la cultiver.

1.2.1 Evaluer et cultiver la culture sécurité

Lors de notre revue de littérature, nous avons identifié plusieurs travaux qui ont tenté d'établir des modèles conceptuels afin de cultiver une culture de sécurité, tels que le modèle de Sherif et Furnell (2015) qui comprend trois sous-modèles : de création, de maintien et d'amélioration d'une culture de sécurité sur la base des résultats de l'analyse de la littérature qui a identifié le soutien de la haute direction, le comportement en matière de sécurité, la conformité et la sensibilisation comme facteurs cruciaux avec d'autres variables qui ont un impact sur l'amélioration continue des processus d'une telle culture.

- **L'étude de Thomson, von Solms, Louw (2006)**

Ces chercheurs proposent un modèle qui s'appelle MISSTEV (Model for Information Security Shared Tacit Espoused Values), sous forme de spirale. Ces auteurs ont mobilisé les modes de connaissance de (Nonaka, 1994) où la création de connaissance consiste à identifier les connaissances existantes et les convertir en nouvelles connaissances. Cela se fait en classant quatre processus d'interaction entre connaissances tacites et connaissances explicites. Ces

processus sont classés comme socialisation, externalisation, combinaison et internalisation. Le modèle MISSTEV est présenté dans la figure suivante :

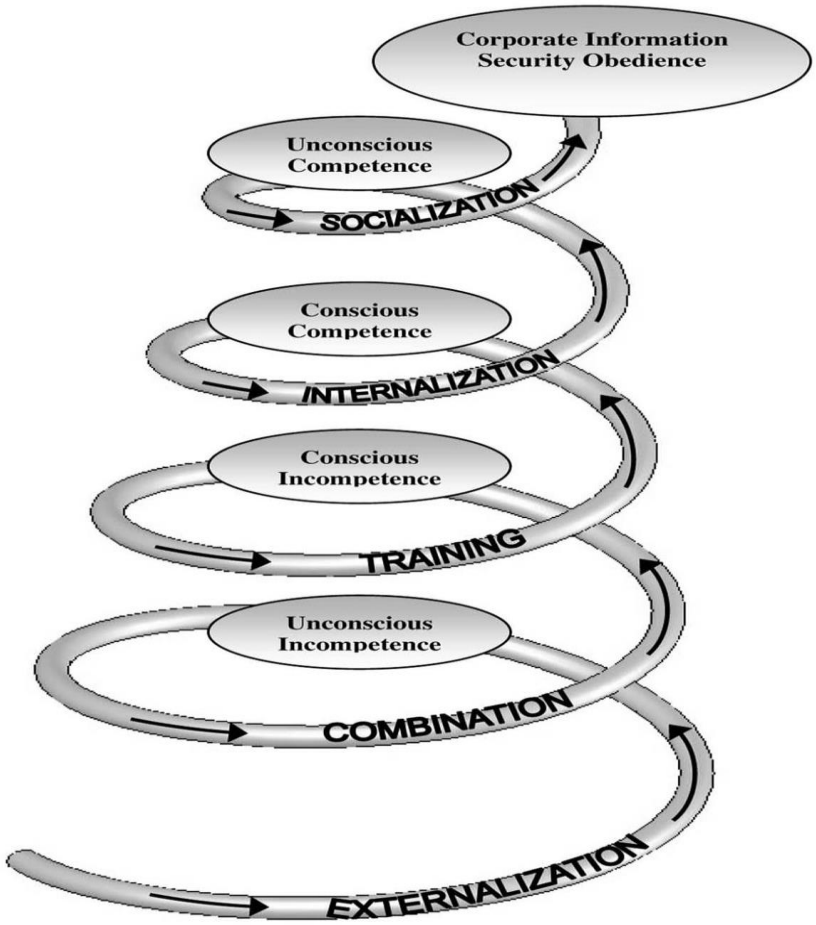


Figure 6 : le modèle de sécurité de l'information valeurs partagées tacites ou MISSTEV de Thomson et al (2006)

À travers le modèle MISSTEV, les employés doivent être informés de la vision de la SSI de la haute direction et leurs rôles et responsabilités de protéger les informations. Pour ces chercheurs, en suivant la spirale de leur modèle, les employés doivent avoir conscience et être formés aux bonnes compétences nécessaires pour protéger les informations et que ces compétences devraient faire partie des pratiques quotidiennes des employés, et que si tous les employés suivent la spirale du modèle MISSTEV (Figure 6), l'obéissance à la sécurité doit devenir évidente dans l'organisation et la vision de la haute direction se réalise.

- **L'étude d'Alnatheer, Chan, Nelson (2012)**

Ces chercheurs proposent un modèle théorique avec des facteurs qui constituent la culture sécurité (Conscience et propriété de la sécurité) et des facteurs qui influencent cette culture sécurité (Support de la direction, politique de sécurité, formation à la sécurité). Ils ont mené une enquête avec 254 répondants de 64 organisations saoudiennes pour valider leur modèle :

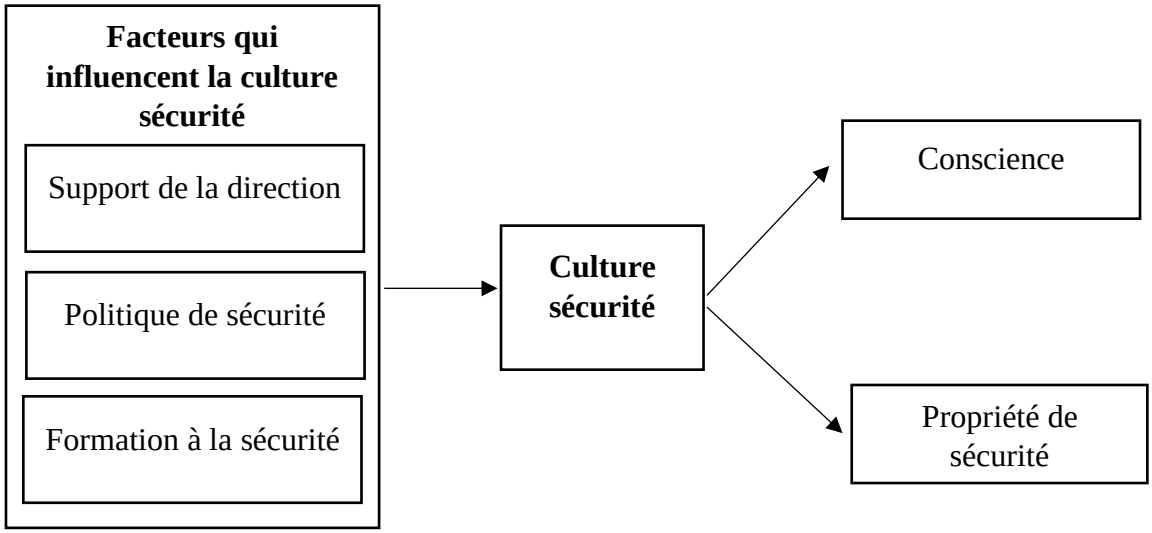


Figure 7 : Modèle de la CSSI d'Alnatheer et al (2012)

Ces chercheurs ont mobilisé une étude qualitative par le biais des entretiens dans huit organisations avec huit experts en sécurité de l'information avant de procéder à l'enquête à plus grande échelle. Leur étude qualitative a révélé la culture sécurité comme le reflet de la conscience et la propriété de sécurité et que les facteurs qui influencent cette culture sécurité sont : l'implication de la haute direction, l'application d'une politique de sécurité ainsi que la formation à la sécurité. Ensuite, ils ont validé leur modèle par une enquête quantitative.

- **L'étude de N. Martins and A. Da Veiga (2015)**

Ces auteurs ont établi un modèle de la CSSI avec quatre mécanismes : management, politiques, sensibilisation et conformité qui peuvent influencer positivement sur la culture de la sécurité. Leur modèle est basé sur le questionnaire ISCA (Information Security Culture Assessment) et validé par modélisation d'équations structurelles (SEM) à l'aide de données empiriques dérivées à partir d'une évaluation ISCA. Avec la participation de 2 159 employés de 12 pays différents, ils ont pu confirmer que le management, les politiques, la sensibilisation et la conformité contribuent à une positive culture SSI. Leur modèle est présenté dans la figure suivante :

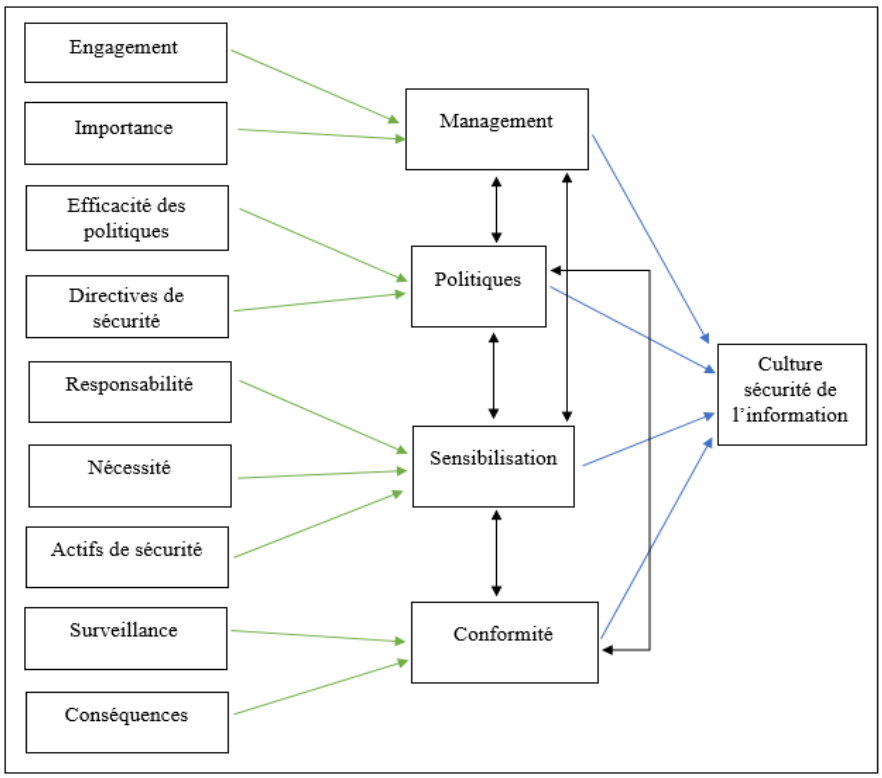


Figure 8 : Modèle de la CSSI de Martins et Da Veiga (2015)

Mécanismes influençant la CSSI	Description
Management (Hu, Dinev, Hart, & Cooke, 2012; Johnson & Goetz, 2007; Knapp, Marshall, Rainer, & Ford, 2006; Wilderom, Van den Berg, & Wiersma, 2012)	Le management ou le leadership dans l'organisation jouent un rôle essentiel dans la formation de la culture souhaitée. Ils doivent définir la stratégie de la SSI de l'organisation et donner l'exemple.
Politiques de SSI (Vroom et Von Solms 2004, ISF 2000, Boxand Pottas 2013)	Connaissance et perception des informations par les employés, les règles et procédures de la politique de sécurité pourraient influer sur la CSSI de manière positive. La politique de sécurité des SI est une pierre angulaire essentielle pour la culture de la sécurité du SI et sert de base pour créer des valeurs et des croyances communes.
Sensibilisation et formation (Nosworthy 2000, Thomson et Al. 2006, Parsons et al. 2014, Herold 2011, Da Veiga et Martins 2015)	La sensibilisation à la SSI et la formation sont mis en œuvre pour éduquer les employés à comprendre le risques et aux contrôles pertinents à utiliser et à respecter. Il a été prouvé que la formation et la sensibilisation ont un impact positif sur la CSSI.
Conformité (Parsons et al. 2014)	La connaissance des politiques et procédures par les employés a un impact positif sur l'attitude envers les politiques de SSI et la conformité. Dans une organisation où il existe une forte CSSI, on pourrait attendre la conformité en tant que trait visible de la culture.

Tableau 6 : Facteurs influençant la CSSI (Martins and A Da Veiga 2015)

Construit (Sous-dimension)	Description
Engagement	Engagement d'une organisation et point de vue des employés concernant la protection des informations.
Importance	L'importance perçue de la sécurité du SI par le management qui comprend des cadres.
Efficacité des politiques	Évaluer si la politique de sécurité est compréhensible et si elle a été communiquée avec succès.
Directives de sécurité	La perception de savoir si l'organisation a des directives claires pour la protection des informations des employés et des clients.
Responsabilité	Responsabilité de la sécurité du SI d'une perspective de l'utilisateur final.
Nécessité	La nécessité de la sécurité du SI est établie en se concentrant sur des concepts spécifiques tels que : les personnes, le temps, l'argent et l'impact des changements.
Actifs de sécurité	Évalue la perception des utilisateurs de la protection des actifs d'information sur support papier et électronique.
Surveillance	La perception du contrôle et suivi d'actions.
Conséquences	Les mesures prises en cas de non-respect.

Tableau 7 : Les construits de l'ISCA (N. Martins and A. Da Veiga 2015)

Ces deux auteurs ont essayé de comprendre l'influence des différents construits (sous-dimensions) dans ISCA (Information Security Culture Assessment). L'ISCA comprend 45 déclarations réparties sur neuf construits (Tableau 7). Les flèches vertes (Figure 8) décrivent les constructions ISCA qui pourraient influencer les facteurs identifiés dans le tableau 6 qui, à leur tour, pourraient influencer la CSSI. Les résultats de leur étude montrent que la direction a une influence positive sur les politiques de sécurité, et à leur tour les politiques ont une forte influence sur la sensibilisation. Cette dernière a une influence positive et forte sur la conformité. Et finalement, ils ont montré que le management ou la direction, les politiques, la sensibilisation et la conformité contribuent à l'évaluation de la CSSI.

- **Modèle holistique de Tolah, Furnell, Papadaki (2017)**

Cette étude propose un cadre holistique de la CSSI avec une distinction entre les facteurs qui constituent et les facteurs qui influencent cette culture sécurité. Cette classification a été proposée auparavant par Alnatheer et al en 2012. Ils ont proposé un cadre qui tient compte des principaux facteurs humains clés associés à la CSSI suggérée par des cadres antérieurs et ajoutent de nouveaux facteurs pour voir le lien potentiel entre ces facteurs et la CSSI. Selon ces

auteurs, ce cadre permet à la fois d'améliorer et d'évaluer la culture sécurité. Leur cadre est présenté dans la figure suivante avec les facteurs expliqués dans le tableau 8 :

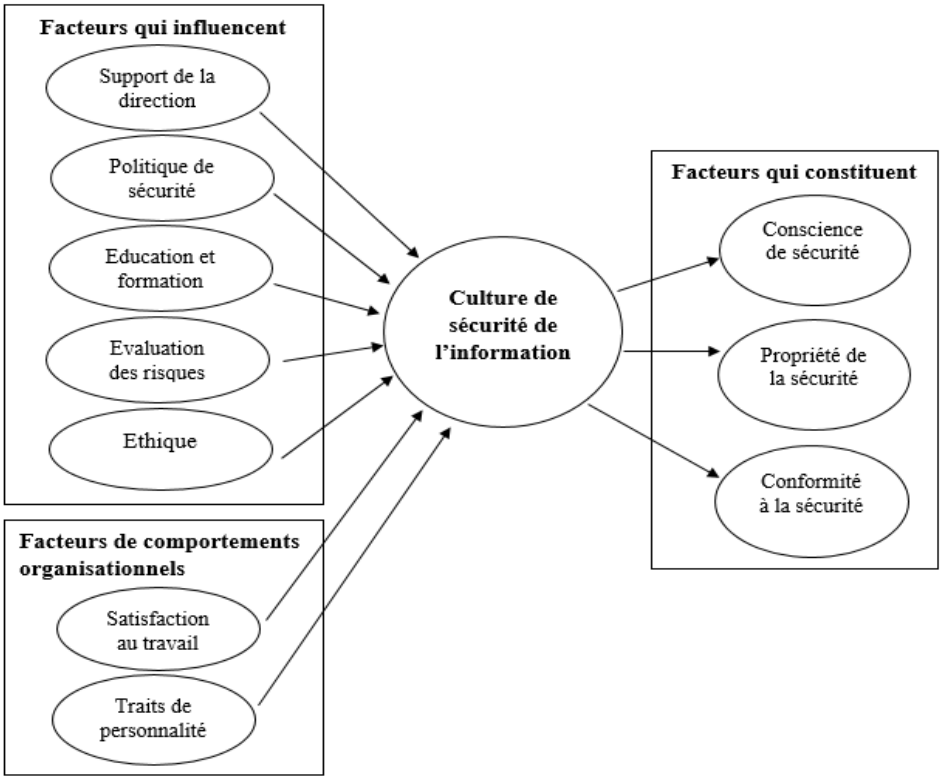


Figure 9 : Modèle holistique de la CSSI de Tolah et al (2017)

Facteurs	Description
Support de la direction (Martin et Da Veiga, 2015)	fait référence à un degré de compréhension par la haute direction de l'importance de la fonction de sécurité du SI et participe aux activités liées à la sécurité pour améliorer et créer une forte culture de sécurité du SI
Politiques de sécurité (Da Veiga, 2015)	est un document écrit qui précise les stratégies de l'organisation et les exigences de la sécurité, une approche qui guide à la fois la gestion et le comportement des employés
Education et formation (Da Veiga et Martins, 2017)	est un processus d'apprentissage qui fournit des connaissances d'un certain sujet lié à l'environnement de la sécurité et les compétences de sécurité requises pour que les employés exécutent les procédures de sécurité
Analyse et évaluation des risques (Da Veiga et Eloff, 2010; Martins et Eloff, 2002)	définit quand les contre-mesures sont suffisantes pour diminuer la probabilité de perte et aide les organisations et leurs employés à devenir capables de comprendre les dommages potentiels à la sécurité, ce qui contribue à créer une prise de conscience de la culture sécurité du SI
Éthique (Alnatheer et al. 2012; Martins et Eloff, 2002)	fait référence aux valeurs et aux règles qui aident à distinguer les droits par une organisation

Traits de personnalité (McCormac et al. 2017)	décrit les facteurs de personnalité, leurs facteurs potentiels et aide à comprendre la variabilité entre les individus pour comprendre les mécanismes psychologiques sous-jacents qui pourraient affecter le comportement des utilisateurs en matière de sécurité du SI
Satisfaction au travail (D'Arcy et Greene, 2009).	fait référence au sentiment général de «bien-être» sur le lieu de travail et aide à déterminer comment un employé peut s'adapter à des facteurs situationnels, tels que le maintien de son engagement, ce qui peut nuire aux organisations
Conscience de sécurité (Da Veiga et Martins, 2017)	définit quand les utilisateurs comprennent les problèmes potentiels liés à la sécurité du SI et prennent conscience de leur mission de sécurité qui conduit à l'engagement envers l'idéal
Propriété de la sécurité (Alnatheer et al. 2012)	fait référence à la façon dont les employés perçoivent leurs responsabilités, leurs rôles dans la sécurité et leur volonté d'agir de manière positive pour améliorer leur propre performance en matière de sécurité et la performance de l'organisation
Conformité à la sécurité (Furnell and Thomson, 2009; Da Veiga and Martins, 2017)	fait référence à la manière dont le comportement des employés est conforme aux politique de sécurité, réglementations et pratiques de sécurité afin de réduire les failles de sécurité causées par la mauvaise conduite des employés, ainsi que d'améliorer la culture de la sécurité du SI au sein des organisations

Tableau 8 : Les facteurs du modèle holistique de Tolah et al (2017)

1.2.2 Les trois niveaux de la culture sécurité de Schlienger et Teufel (2003)

Initiant ce qui va fonder le raisonnement en « couches », raisonnement très souvent utilisé en management interculturel, E. Schein (1985) distingue trois niveaux qui permettent d'identifier une culture au sein d'une organisation : les artefacts, les valeurs et les hypothèses fondamentales. Par analogie à ces trois niveaux de culture établie par Schein, les travaux de Schlienger et Teufel (2002) présentent les trois niveaux de la culture avec des exemples dans le domaine de la sécurité de l'information. Ces niveaux et leurs interactions sont représentés dans le schéma suivant :

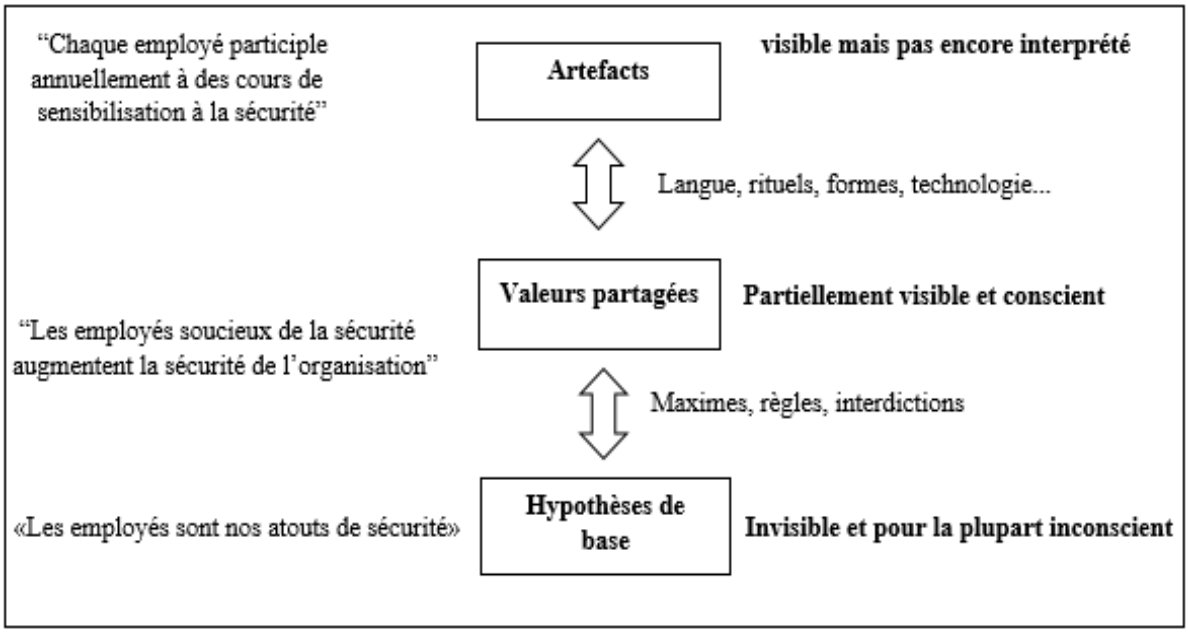


Figure 10 : Les trois niveaux de la culture sécurité avec des exemples de culture de sécurité de l'information de Schlienger et Teufel (2002) adapté de (Schein 1985)

Donc, en se référant à Schein et son modèle des trois niveaux de culture, Schlienger et Teufel déduisent que la culture sécurité est de même, formée de trois niveaux qui sont les artefacts, les valeurs et les hypothèses fondamentales liées aux questions de sécurité de l'information au sein de l'organisation. Ils définissent ces trois niveaux comme suit :

-Les artefacts : c'est ce qui se passe réellement dans l'organisation. Sans les compétences nécessaires, il serait impossible d'exécuter correctement les tâches liées à la sécurité. Ainsi, pour que les activités quotidiennes se déroulent de manière sécurisée, les utilisateurs doivent avoir une connaissance suffisante de la manière de s'acquitter de leurs actions en toute sécurité ;

-Les valeurs partagées *:* sont les principes sociaux, les philosophies, les objectifs, les normes et les croyances considérés comme ayant une valeur intrinsèque pour les membres de l'organisation. C'est par exemple un document de politique de sécurité qui inclut les règles à adopter par tous en matière de sécurité ;

-Les hypothèses de bases *:* ce niveau regroupe les croyances et les valeurs de base de chaque employé. Si une telle croyance devait entrer en conflit avec l'une des valeurs adoptées, il pourrait être essentiel de savoir pourquoi un contrôle spécifique est nécessaire pour garantir la conformité.

Les deux substances fondamentales de la culture organisationnelle sont les hypothèses et les croyances de base. La culture organisationnelle s'exprime par conséquent dans les valeurs collectives, les normes et les connaissances des organisations. À leur tour, ces normes et valeurs collectives affectent le comportement des employés. Les artefacts et les créations tels que les manuels, les rituels et les anecdotes sont l'expression de ces normes et valeurs. La culture organisationnelle émerge et se développe avec le temps. Elle est formée par le comportement des membres dominants de l'organisation comme les fondateurs et les cadres supérieurs. Une culture organisationnelle peut avoir différentes sous-cultures basées sur des sous-organisations ou des fonctions. Pour Schlienger et Teufel, la culture de la sécurité de l'information est une sous-culture en ce qui concerne les fonctions générales de l'entreprise. Elle devrait soutenir toutes les activités de telle manière, que la SSI devient un aspect naturel dans les activités quotidiennes de chaque employé.

Selon Schlienger et Teufel, (2002) la CSSI se concentre sur les aspects socioculturels de la gestion de la SSI. Pour construire une CSSI, ils se sont inspirés du groupe consultatif international sur la sûreté nucléaire (Brandao 1994). Après la catastrophe de Tchernobyl, ils ont défini le concept de culture de la sûreté (International Nuclear Safety Advisory Group, 1986 ; Freitag 1994). Avec peu de modifications, ces auteurs ont adapté cette culture de la sûreté à la culture de la sécurité de l'information. Les mesures de la culture de sécurité ciblent principalement la couche de normes, de valeurs et de connaissances. Selon ce modèle, la culture de sécurité doit définir trois niveaux de responsabilité (Figure 11) :

1. Politique d'entreprise

2. Gestion

3. Individuels

Ces couches sont entourées par les conditions de base externes ainsi que par les normes et valeurs sociales qui, par exemple, sont exprimées dans le droit national et international. Au niveau de la politique d'entreprise, la SSI doit être définie comme une cible d'entreprise. Cela signifie que la direction est responsable de définir la politique de sécurité. Par conséquent, ils doivent fournir des ressources suffisantes pour mettre en œuvre cette politique. Cette tâche pourrait être déléguée, par exemple à un responsable de la sécurité (RSSI), mais la direction dans son ensemble reste responsable. Un RSSI peut être positionné à plusieurs endroits de l'organigramme: dans le service informatique, dans une nouvelle unité du personnel ou dans un service de sécurité existant.

Pour ces chercheurs, les différents chefs de service sont responsables de la conformité de la politique de SSI et de sa mise en œuvre dans leurs unités. Ils doivent être suffisamment motivés pour respecter la politique de sécurité; car sans leur aide, il n'est pas possible de mettre en œuvre une telle politique. Pour mettre en œuvre cette politique de sécurité, la direction doit définir et contrôler les différentes mesures de sécurité. De plus, ils doivent se qualifier et former leurs employés. Un comportement conforme à la sécurité doit être attribué, et les violations de sécurité malveillantes doivent être poursuivies. En outre, la stratégie de sécurité doit être vérifiée et évaluée régulièrement.

Au niveau individuel, chaque collaborateur doit contribuer à la sécurité de l'organisation elle-même. Il doit avoir une attitude critique, en demandant:

- Ai-je compris ma tâche?
- Quelles sont mes responsabilités?
- Ai-je suffisamment de connaissances pour accomplir ma tâche?
- Ai-je besoin d'aide?

Il / elle doit agir avec prudence et diligence raisonnable. Les comportements anormaux des personnes ou des systèmes informatiques, y compris les dysfonctionnements, doivent être enregistrés et signalés. En outre, l'utilisateur doit être intégré dans le processus d'analyse des risques et l'entreprise doit installer un système de suggestion des employés. (Schlienger et Teufel, 2002).

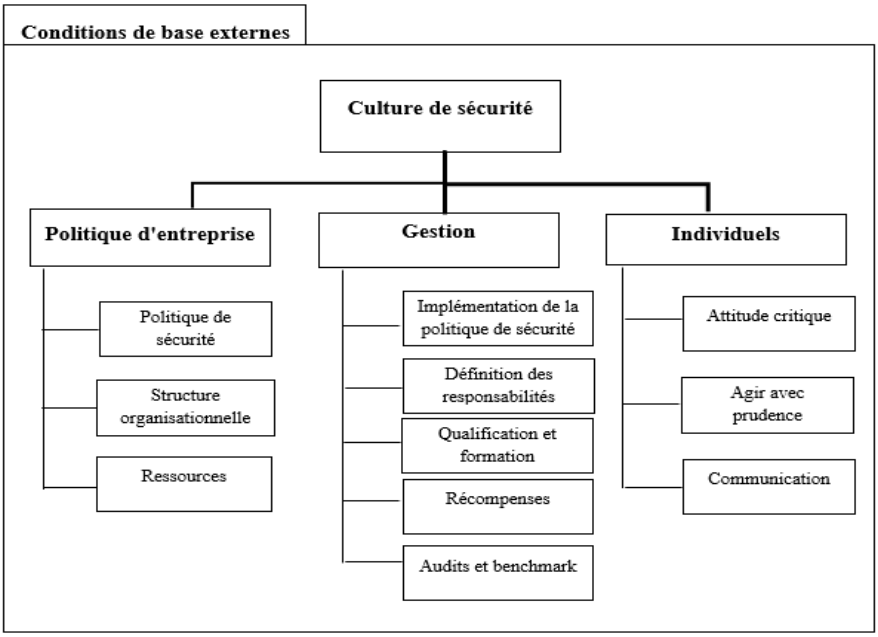


Figure 11 : Les couches de la culture sécurité de (Schlienger et Teufel, 2002)

Pour ces auteurs, concevoir un processus de sécurité et mettre en œuvre une technologie de sécurité devrait commencer par le processus métier et les utilisateurs. La combinaison de la technologie et de la conscience et de la qualification humaine peut améliorer considérablement le niveau de sécurité global d'une organisation. La sécurité devrait devenir aussi naturelle que l'air. Pour atteindre cet objectif, il est nécessaire d'avoir une culture de la sécurité qui aborde les aspects socioculturels de la sécurité.

1.2.3 Synthèses des construits proposées dans la culture sécurité

La revue de littérature réalisée sur la culture sécurité, nous a permis d'identifier les construits d'une culture sécurité ce qui permet de mieux comprendre quels facteurs peuvent influencer la culture sécurité et quels facteurs constituent cette culture.

Recherche	**Construits**
Martin et Eloff (2002)	Politique, benchmark, analyse des risques, budget, gestion, confiance, sensibilisation, conduite éthique, changement.
Chia et al. (2002)	Budget de sécurité, dépenses de sécurité, sensibilisation des employés à la sécurité, risque de sécurité du personnel, mise en œuvre de la politique de sécurité, suggestions de sécurité, propriété de la sécurité, audits.
Helokunnas et Kuusisto (2003); Kuusisto et Ilvonen (2003)	Cadre de culture de sécurité (normalisation, certification, mesures de la sécurité du SI). Composantes du contenu (attitude des gens, motivation, connaissances, communication, conformité).
Schlienger et Teufel (2003, 2005)	La culture de sécurité comprend trois niveaux: Les politiques d'entreprise (politique, structure organisationnelle, ressources); Gestion (mise en œuvre de la politique de sécurité, responsabilité, qualification et formation, récompenses et poursuites, audits, benchmarks); Individuel (attitude, communication, conformité).
OECD (2005)	Sensibilisation, responsabilité, réponse, éthique, démocratie, évaluation des risques, conception et mise en œuvre de la sécurité, gestion et réévaluation de la sécurité.
Tessem et Skaraas (2005)	Plan à long terme, gestion du changement, top management, participation, l'image de marque, culture organisationnelle.
Ruighaver et al. (2007)	Cadre de gouvernance de la sécurité (mécanisme structurel, mécanismes fonctionnels, participation sociale) Influences sur la dimension du cadre de la culture de sécurité (contrôle, coordination, appropriation, responsabilité).
Dojkovski et al. (2006)	E-learning individuel et organisationnel; éthique; culture nationale et organisationnelle; gestion (politiques et procédures, benchmark, analyse des risques, budget, gestion, réponse, formation, éducation, sensibilisation, gestion du changement);

	Comportementale (responsabilité, intégrité, confiance, appartenance ethnique, valeurs, motivation, orientation croissance personnelle).
Kraemer et Carayon (2007)	Participation des employés, formation, pratiques d'embauche, système de récompense, engagement de la direction, communication et rétroaction.
Da Veiga & Eloff (2010)	Leadership et gouvernance (parrainage, stratégie, gouvernance informatique, évaluation des risques, ROI / métriques / mesure); Gestion et organisation de la sécurité (juridique et réglementaire, organisation de programmes); Politique (politiques, norme, procédure, lignes directrices, meilleures pratiques, certification); Gestion du programme de sécurité (surveillance, audit, conformité); Gestion des utilisateurs (sensibilisation, formation, confiance, confidentialité, conduite éthique); Protection et opérations technologiques (développement de systèmes, exploitation technique, physique et environnement, gestion des actifs, gestion des incidents, continuité des activités); Gestion du changement.
Alnatheer et al. (2012)	Les facteurs influencent la CSSI (direction, application des politiques, éducation et formation aux SI) Les facteurs constituant la CSSI (Sensibilisation à la sécurité, propriété de la sécurité).
AlHogail et al. (2015)	Dimension organisationnelle: gestion (politique, pratique, communication); Environnement (culture nationale, normes et réglementations, culture organisationnelle); Dimension employée: préparation (sensibilisation et formation, changement); responsabilité (récompense, suivi et contrôle, acceptation).
Sherif et al. (2015)	Culture nationale; la culture organisationnelle; Conformité à la sécurité (comportement du SI, soutien de la direction, politique, sensibilisation et éducation, acceptation).
Tolah et al (2017)	Facteurs qui influencent la CSI : Support de la direction, Politique de sécurité, Education et formation, évaluation des risques, Ethique ; Facteurs de comportements organisationnels : Satisfaction au travail, traits de personnalité ; Facteurs qui constituent la CSI : Conscience de sécurité, propriété de sécurité, conformité à la sécurité.

Tableau 9 : Résumé des construits proposées dans la culture sécurité

Adapté de Tolah et al (2017)

2. La culture sécurité au cœur de la gouvernance des systèmes d'information (GSI)

2.1 La gouvernance des systèmes d'information (GSI)

Weill et Ross, (2004) définissent la GSI comme un processus de pilotage qui vise à maîtriser les décisions à prendre ainsi que les risques sous-jacents et à orienter les décisions en vue d'augmenter la valeur et de minimiser les risques pour l'organisation.

La GSI a pour objectif d'améliorer le fonctionnement des SI des organisations. Elle concerne non seulement la DSI mais aussi tous les métiers de l'entreprise qui concourent à la création de valeur grâce aux SI. (Hallépée, 2013).

Au sein de la gouvernance de l'entreprise, la GSI soutient à la fois la gouvernance institutionnelle (focalisée sur la conformité et le contrôle et assure la légalité et la responsabilité) et la gouvernance d'activité (focalisée sur la création de valeur et facilite le processus de prise de décision), le schéma suivant présente la relation entre la GSI et la gouvernance de l'entreprise :

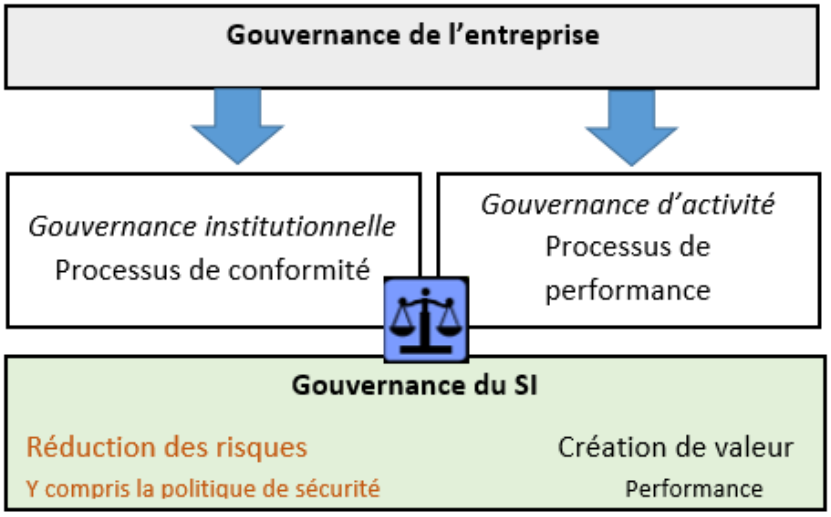


Figure 12 : Relation entre gouvernance de l'entreprise et gouvernance des SI adapté de l'institut de la gouvernance des SI (2005)

L'association ISACA (Information Systems Audit and Control Association) définit cinq piliers pour la GSI, présentés dans la figure suivante et expliqués ci-dessous :

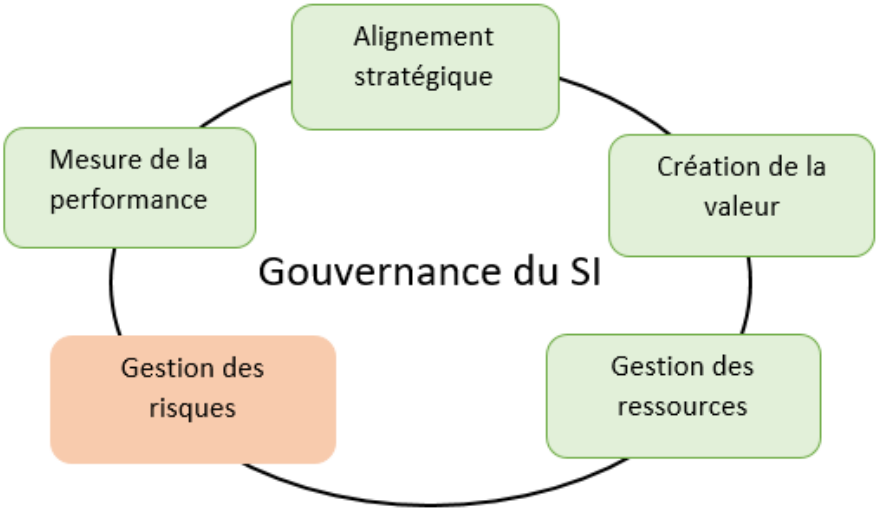


Figure 13 : Les cinq piliers de la gouvernance des systèmes d'information (ISACA)

- **Alignement stratégique :**

Pour une meilleure gouvernance, le système d'information doit être aligné sur la stratégie générale de l'entreprise. Autrement dit, les objectifs du SI doivent être en adéquation avec les grands objectifs stratégiques. La partie « Stratégie des services » du référentiel des bonnes pratiques ITIL[9] s'intéresse à la définition des services adaptés à la stratégie de l'entreprise. Il existe plusieurs modes d'alignement qu'on peut trouver dans le modèle d'Henderson et Venkatraman (1993), qui propose 4 formes distinctes d'alignement stratégique du SI.

- **Création de la valeur :**

Le SI doit créer de la valeur et doit apporter des bénéfices à l'entreprise, son budget a un double objectif : il doit servir à mettre en évidence la valeur créée à travers les informations qu'il possède et permettre d'optimiser les coûts. La valeur ajoutée demeure en quelque sorte abstraite et difficile à mesurer.

- **Gestion des risques :**

La gestion des risques consiste à identifier en premier lieu, l'ensemble des menaces auxquelles est exposé le SI et essayer dans la mesure du possible de les contrôler. Dans ce contexte,

[9] Information Technology Infrastructure Library : ensemble d'ouvrages recensant les bonnes pratiques du management du système d'information.

l'ensemble des référentiels ISO 27000 s'intéressent au management de la sécurité du système d'information.

- **Gestion des ressources :**

Ce pilier vise à optimiser et à rationaliser les investissements dans les ressources informatiques (infrastructures, applications, compétence, etc.). Si la fonction SI manque de compétences ou d'infrastructures à sa disposition, cela peut freiner la performance de l'entreprise dans la mesure où la réponse aux besoins des métiers n'est pas efficiente.

- **Mesure de la performance :**

Le SI est un pilier dans la mesure de la performance d'une entreprise, autrement dit dans la surveillance de l'activité et le contrôle de l'aboutissement à l'atteinte des objectifs stratégiques de l'entreprise par le biais de tableaux de bords et d'indicateurs pertinents. La méthode du Balanced Scorecard (tableau de bord équilibré) présente une façon qui vise à mesurer les activités d'une entreprise selon quatre axes : client, processus, apprentissage, finances. La performance est au centre des préoccupations des DSI. C'est le résultat de la maîtrise de la maturité des processus métier et SI (Ravichandran et Lertwongsatien, 2005). Aussi, l'application de méthodes orientées par la maturité des processus comme COBIT[10]ou CMMI[11] est pertinente. Ces cadres proposent un ensemble prédéfini d'objectifs à atteindre et de métriques pour mesurer la maturité des processus. (Claudepierre, 2010).

2.2 Les approches de la gouvernance des SI

Ce titre est dédié à la présentation de quatre approches pour la GSI. Ce sont les approches les plus citées en matière de pratique de la gouvernance des SI : Cobit, COSO, ITIL, CMMi. Nous allons décrire brièvement ces approches ci-dessous :

2.2.1. CobiT : Control Objectives for information and technology

CobiT a été développé en 1994 (et publié en 1996) par l'ISACA (Information Systems Audit and Control Association). C'est un cadre de contrôle qui vise à aider le management à gérer les risques (sécurité, fiabilité, conformité) et les investissements. CobiT est un ensemble de

[10] Control Objectives for Information and related Technology
[11] Capability Maturity Model Integrated

recommandations et de processus permettant d'évaluer les ressources du SI. Il a pour objectif de guider les praticiens dans la mise en place des contrôles internes. (Moisand et Garnier de Labareyre, 2009).

2.2.2. COSO : The Committee of Sponsoring Organizations of the Trendway Commission

COSO est une méthode de gestion de risques. Cette méthode a pour objectif de guider les praticiens dans l'identification des risques associés aux objectifs de rendement et de croissance. (Moeller, 2007). COSO est ainsi un cadre qui permet de gérer les risques à tous les niveaux de l'entreprise, et pas uniquement de sa composante SI.

2.2.3. ITIL : IT Infrastructure Library

ITIL se positionne sur la gestion des services TI, il a pour objectif de guider, par les bonnes pratiques, les professionnels des SI dans la gestion efficace des ressources et l'obtention de la qualité des services informatiques. (Chamfrault, 2006). ITIL permet, grâce à une approche par les processus, d'améliorer la qualité des SI et de l'assistance aux utilisateurs en créant la fonction centre de services qui centralise et administre l'ensemble de la gestion des SI.

2.2.4. CMMI : Capability Maturity Model Integrated

CMMi se positionne sur l'évaluation de la maturité des processus de gestion des projets (Chrissis et al, 2008), (SEI[12], 2006). Le CMMi a pour objectif d'amener une organisation à optimiser l'efficacité et la qualité de ses processus. Il se compose des bonnes pratiques issues des modèles de maturité CMMSE (ingénierie des systèmes), CMM-SW (ingénierie des logiciels), CMM-IPD (développement des produits) et CMM-SS (gestion des fournisseurs).

2.3 Gérer les risques pour améliorer la culture sécurité et créer de la valeur

La sécurité d'un SI revient à essayer de se protéger contre les risques liés à l'informatique qui peuvent avoir un impact sur la sécurité de celui-ci, ou des informations qu'il traite. (Ikkou et Elouidani, 2016). Cette sécurité est basée sur la gestion des risques, qui doit garantir la protection du patrimoine informationnelle de l'entreprise.

L'ISO[13] définit la gestion des risques comme l'ensemble des activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque. Nous dégageons en général trois finalités à la gestion des risques pour les SI : améliorer la sécurisation des systèmes d'information, justifier

[12] Software Engineering Institute de l'université Carnegie Mellon, Pittsburgh, États-Unis
[13] ISO/IEC Guide 73:2002, Risk management – Vocabulary – Guidelines for use in standards.

le budget alloué à la sécurisation du système d'information, prouver la crédibilité du système d'information à l'aide des analyses effectuées.

Pour Mayer et Humbert (2006), la gestion des risques se compose de trois blocs interdépendants. Ils distinguent en premier lieu les ressources et les besoins de sécurité, ensuite les risques pesant sur ces ressources et enfin, les mesures prises ayant pour but de traiter les risques et donc d'assurer un certain niveau de sécurité.

Les méthodes de gestion des risques de sécurité sont des outils méthodologiques, qui aident les organisations à prendre des décisions rationnelles sur la sécurité de leur SI. (Moisand et Garnier de Labareyre, 2009).

Une gouvernance centrée sur les risques permet aux dirigeants de l'entreprise d'employer la gestion du risque informatique comme un levier de résilience, mais aussi comme un bouclier de protection de la technologie et de l'infrastructure physique, et donc au final, comme un facteur de dynamisation de la croissance (IBM, 2008).

Gerber & von Solms (2005) ont également proposé un processus d'analyse holistique des risques basé sur l'entreprise afin d'élargir et de soulever la question de la sécurité du SI à un problème d'alignement stratégique de l'entreprise. Les résultats d'une analyse des risques peuvent motiver une attitude proactive envers la gestion de la sécurité du SI (Dojkovski et al, 2006).

La politique de sécurité indique l'ensemble des mesures à prendre, des structures à définir et l'organisation à mettre en place afin (Longeon et Archimbaud ,1999):

-D'empêcher (au moins freiner) la détérioration, l'utilisation anormale ou la pénétration des systèmes et réseaux ;

-De détecter toute atteinte, malveillante ou non, à l'intégrité, la disponibilité et la confidentialité des informations ;

-D'intervenir afin d'en limiter les conséquences et le cas échéant, poursuivre l'auteur du délit.

Si nous tiendrons en compte de l'importance des systèmes d'information dans les entreprises, il n'est pas surprenant d'apprendre qu'elles courent d'énormes risques lorsque leurs systèmes ne sont plus disponibles. Perreault (2012), a essayé de calculer le coût d'un incident à partir des éléments à considérer pour établir les pertes associées à un incident : perte de réputation (impliquer l'équipe de marketing), frais de campagne de marketing pour récupérer la part de

marché perdu, perte de confiance des investisseurs (réduction de la valeur des actions), perte de ventes (impliquer l'équipe de vente), perte de productivité des ressources impactées par l'incident , perte d'avantages compétitifs, frais légaux (avocats, dédommagements) poursuite(s) criminelle(s), augmentation des primes d'assurance, frein au développement de nouveaux projets, frais de consultation, coûts des ressources assignées à résoudre l'incident et dommage aux actifs informationnels.

Une autre enquête faite sur dix organisations par Dagorn (2008), montre que pour neuf organisations, les principaux enjeux liés à la sécurité (en termes de conséquences en cas de compromission de la sécurité), sont la perte de crédibilité ou de confiance ; huit organisations craignent la perte de marché ou la perte d'argent, quatre redoutent le recours juridique (tribunaux, etc.), trois soulignent la perte de temps, et une organisation ajoute d'autres enjeux tels que la perte d'image.

La gouvernance de la SSI est une approche stratégique de la sécurité visant à la protection des actifs informationnels[14] de l'organisation, dans une acceptation allant au-delà de la « simple » garantie opérationnelle que les informations de l'organisation sont adéquatement protégées : elle implique une vision holistique du management de la sécurité du SI, en prenant en compte les enjeux, les décisions, la stratégie globale et à long terme, qui ne font pas partie des missions du technicien (Dagorn et Poussing, 2012), ce qui impose une gestion des risques et une prise en compte des questions de SSI au plus haut niveau de l'organisation.

Dans ce contexte, la gouvernance de la SSI prend son sens, puisqu'elle « *consiste à mettre en place une structure permettant de prendre les bonnes décisions en matière de sécurité, au bon moment et au bon niveau hiérarchique* » (Fernandez-Toro, 2009). Elle permet aux organisations d'inclure les questions de sécurité dans leur stratégie de gouvernance globale. Mais l'intérêt d'une gouvernance de la sécurité du SI s'explique également par la prise de conscience des dirigeants, de l'impact profond que peuvent avoir les questions de sécurité sur le bon fonctionnement et la performance du système d'information (SI) de l'organisation (Dagorn et Poussing, 2012).

Ces deux auteurs Dagorn et Poussing, (2012), ont réalisé une étude sur 120 organisations, et les résultats de leur étude confirment que la gouvernance de la sécurité du SI est un sous-ensemble à part entière de la gouvernance des SI, puisque les organisations impliquées dans les deux

[14] Sapir (2005, p. 159) définit un actif informationnel comme « *une information considérée comme simultanément pertinente et utilisable pour une décision donnée* ».

démarches sont exactement les mêmes. Soulignons aussi que la responsabilité de la gouvernance de la sécurité est attribuée, selon les organisations, à des acteurs variés allant du responsable SI (DSI), *risk manager*, responsable qualité/conformité, RSSI, au directeur général.

Cette étude montre que le rattachement de la gouvernance à la DSI concerne plutôt les organisations faiblement ou moyennement exposées aux risques liés à l'information, où la fonction sécurité a une vocation plus opérationnelle que stratégique. Le rattachement de la gouvernance au management des risques à l'audit ou au contrôle interne est plutôt typique des organisations exposées aux risques liés à l'information (secteurs d'activités tertiaires et quaternaires), et le rattachement de la gouvernance à la direction générale de l'organisation est privilégié lorsque l'information est le produit de l'organisation, et que le risque de l'organisation et celui lié à l'information sont fortement liés.

Pour Dagorn et Poussing, (2012), les déterminants proposés du processus d'engagement des organisations dans la gouvernance de la sécurité du SI sont très proches des quatre déterminants identifiés par Venkatesh et al. (2003) :
(1) la performance espérée de la démarche de gouvernance (valeur ajoutée, bénéfices, avantage concurrentiel) ;
(2) l'effort déployé pour sa mise en œuvre (dépassement des freins, obstacles) ;
(3) les conditions facilitatrices (connaissance d'organisations susceptibles d'aider l'organisation dans sa démarche) ;
(4) l'influence sociale (normes subjectives, image, valeurs).
Plusieurs auteurs tels que Theys (2003), Bodet et Lamarche (2007) soulignent que la gouvernance est une forme d'innovation. Dans le domaine des SI, Bidan et Trinquecoste (2010) mettent en lumière l'intérêt du triptyque « gouvernance– innovation – TI ».

La sécurité a été assimilée à une innovation dans plusieurs travaux, comme par exemple, les travaux de Kesh et Ratnasingam (2007) qui parlent d'une innovation exclusivement technique, alors que Herath et al. (2010) évoquent une innovation technique et organisationnelle. De même, la perception des utilisateurs est régulièrement prise comme cadre d'analyse des innovations technologiques de sécurité comme dans les travaux : Charndra et Calderor, (2005) ; Cazier et al. (2008). Nous concluons alors, que la gouvernance de la sécurité des SI peut être appréhendée à la fois comme une innovation technique et organisationnelle. Fayolle (2017) affirme que l'innovation réussie est toujours une source de valeur nouvelle et conclut que la création de valeur est reliée à l'innovation et à la création d'avantages concurrentiels durables.

Donc, une bonne gouvernance de la sécurité des SI est une source de création de valeur et d'avantage concurrentiel durable pour les organisations.

Si nous revenons à la littérature sur la culture sécurité des SI, plusieurs auteurs ont identifié la gestion des risques (y compris l'analyse et l'évaluation des risques) comme étant un construit d'une mise en place d'une culture sécurité des SI (Martin et Eloff, 2002 ; OECD, 2005 ; Dojkovski et al, 2006, Da Veiga & Eloff, (2010)), pour Tolah et al (2017), ils considèrent l'évaluation des risques comme étant un facteur qui influence la culture sécurité, dans la mesure où les contre-mesures sont adéquates pour réduire la probabilité de perte et aident les organisations et ses employés à devenir capables de comprendre les dommages potentiels à la sécurité, ce qui contribue à créer une prise de conscience de la culture sécurité des systèmes d'information.

Donc nous concluons, qu'une gestion des risques liés aux SI aide à créer une culture sécurité, cette culture va améliorer à son tour la gouvernance de la SSI, ce qui va créer de la valeur pour l'entreprise. Nous allons passer maintenant au titre suivant, qui va présenter l'état des lieux des recherches sur la culture sécurité des SI dans les PME.

3 La culture sécurité des SI (CSSI) dans les PME

Dans le début de notre travail, nous avons mis en lumière la situation des PME et les problèmes que rencontrent ces dernières en ce qui concerne la sécurité des SI. Les PME occupent une place importante dans la plupart des économies. En France, elles constituent la majorité des entreprises et elles éprouvent un retard à se protéger par rapport les plus grandes entreprises.
Après un examen de la littérature dans le domaine de la PME, nous allons dans un premier temps présenter la position particulière qu'occupe la PME dans le monde des entreprises. Dans un deuxième temps, nous allons montrer la place des technologies de l'information et de la communication (TIC) dans ces entreprises. Ensuite, nous discuterons les recherches réalisées dans le domaine de la culture de sécurité du SI dans le cadre des PME. Et finalement, nous allons tenir compte de la place très particulière qu'occupent les dirigeants dans les PME et de leur rôle clé dans le développement d'une culture de sécurité.

3.1. Courants de recherche en PME

Depuis plus de vingt-cinq ans, la recherche en PME n'a cessé de se structurer (Torrès, 1998). Ce chercheur a posé la question suivante : Qu'est-ce qui justifie les chercheurs à s'intéresser

exclusivement aux PME ? Et il a repéré trois types de justifications concernant la recherche en PME :

- Une justification empirique : la PME comme champ d'analyse

Les PME occupent une place importante dans la plupart des économies. La PME constitue un « enjeu de taille » pour amorcer la lutte contre le chômage. Ces entreprises à dimension humaine possèderaient toutes les caractéristiques requises pour s'adapter aux situations de crise : souplesse, dynamisme et flexibilité. Le phénomène PME constitue donc un enjeu économique et justifie de ce fait les études qui lui sont consacrées. L'aspect salutaire de la PME présentée souvent comme « modèle d'adaptation à la crise » s'apparente au phénomène du « *small is beautiful* ».

-Une justification méthodologique : la PME comme outil d'analyse

Par sa faible dimension, la PME est souvent présentée comme une unité productive dont les phénomènes sont plus facilement identifiables, plus lisibles (d'Amboise et Maldowney, 1988). Selon Marchesnay (1993), la recherche en PME permet de faire apparaître « *concrètement, visiblement aux yeux de l'observateur, ce qui est caché, difficile à saisir et à interpréter dans les organisations de grande dimension* ».

-Une justification théorique : la PME comme objet d'analyse

Si la PME est un concept, il convient d'identifier les fondements théoriques qui autorisent le découpage à partir du critère de taille. La réponse à cette question n'est pas neutre sur le plan épistémologique. En effet, selon Cohen. E (1989), la recherche de critères de découpage constitue un des objets de l'épistémologie des sciences de gestion. Ces modes de découpage sont à l'origine d'un processus d'éclatement qui tend à développer des disciplines revendiquant une autonomie- et parfois une hégémonie- parmi les connaissances et les pratiques de gestion.

En prolongeant le raisonnement de Cohen, Torrès, (1998) pose les questions suivantes : peut-on considérer que le mode de découpage selon la taille est de nature à faire de la recherche en PME une véritable discipline des sciences de gestion ? Qu'est-ce qui autoriserait cette discipline à revendiquer un domaine spécifique dans le champ des connaissances théoriques et appliquées des sciences de gestion ? En définitive, n'est-il pas nécessaire de s'interroger sur l'identité de la recherche en PME ? Compte tenu du développement du nombre de chercheurs et de laboratoires qui consacrent leurs travaux exclusivement à la PME, du fait de l'organisation et de la structuration croissantes de ce courant de recherche, ne pourrait-on pas considérer que la

recherche en PME se constitue progressivement en un véritable champ disciplinaire des sciences de gestion ?

Selon Torrès, (1998), il existe plusieurs courants de recherche sur la PME classés en deux types : Les fondements (Le courant de la spécificité et le courant de la diversité) et les prolongements (Le courant de la synthèse et le courant de la dénaturation). Nous allons présenter brièvement, les deux grands courants :

- **Courant de la spécificité :**

À la fin des années 70, la recherche en PME prend un nouvel envol, lorsque plusieurs auteurs ne la considèrent plus comme un modèle réduit de la grande entreprise mais comme une entreprise qui a ses propres particularités: la PME est spécifique (Barreyre, 1967 ; Gervais, 1978 ; Dandridge, 1979 ; Welsh et White, 1981 ; Marchesnay, 1982-a, 1982-b ; Hertz, 1982...). L'entreprise de petite taille devient « la petite entreprise ». La PME se transforme alors progressivement en objet de recherche, mais en objet de recherche relatif dans la mesure où la preuve de la spécificité des petites entreprises ne peut se faire qu'à partir d'études comparatives entre les petites, moyennes et grandes entreprises (d'Amboise et Plante, 1987, Brytting, 1991). Torrès, (1998), considère que l'accumulation et l'intensité des différences mises en évidence entre les petites et les grandes entreprises constituent des signes satisfaisants pour en faire des objets d'une nature différente.
Selon Leclerc, (1990), « *lorsque l'on regarde plus précisément cette entité, on remarque tout d'abord qu'elle n'est appréhendée qu'en termes d'écarts avec les grandes entreprises... La PME-PMI ne prend toujours corps que comparativement à la grande entreprise*. ». Dans ce sens, la PME n'est qu'un objet de recherche relatif, c'est-à-dire que la spécificité des PME n'est pas une thèse en soi mais relative à ce qui la distingue de la grande entreprise. Torrès, (1998), accorde une grande importance à la taille et considère que ce facteur occasionne des changements de nature, et il déduit que la PME est spécifique.
Ce courant de recherche donne une importance accrue à la mise en évidence d'uniformités qui résultent des tendances de la petite taille. Malgré l'hétérogénéité des PME, chaque auteur insiste sur les caractéristiques communes. Ce sont ces invariants qui constituent la base de la spécificité des PME : « *Le monde de la PME, considéré individu par individu, se révèle lui-même d'une extrême complexité ; mais pris en tant que tel, des constantes, des permanences, des tendances en surgissent à l'examen*. » (Julien et Marchesnay, 1988).

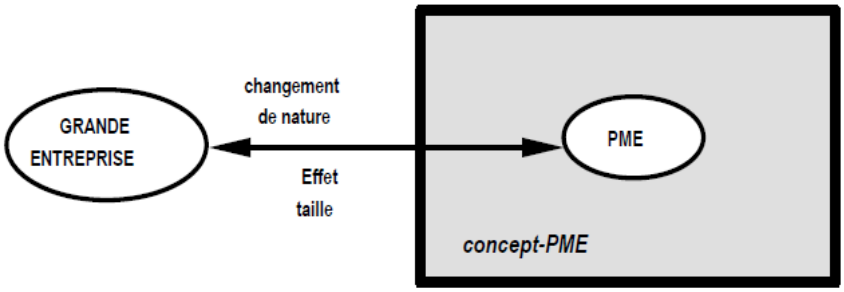


Figure 14 : Le courant de la spécificité Torrès, (1998)

- **Courant de la diversité :**

Ce courant, considère les PME comme un ensemble trop hétérogène pour se prêter à une tentative de généralisation. Il semble difficile voire impossible de les regrouper autour d'un modèle unique. Du fait de la diversité du champ des PME, aucune généralisation n'est possible et tout est affaire de contexte. Dans ces conditions, la PME n'est pas une catégorie homogène mais une appellation commode qui désigne une réalité multiple susceptible de se différencier par l'activité, par les stratégies adoptées, par la forme de propriété, par les modes de gestion... « *On sait qu'il est difficile de parler d'une théorie des PME alors que celles-ci sont extrêmement hétérogènes....on ne peut donc échapper à une approche de contingence*. » (Julien, 1994). Pour Bayad et Nebenhaus (1994), « *Contrairement aux Grandes Entreprises, pour les PME il est difficile de mettre en évidence des invariants de gestion* ». Enfin, pour Mahe de Boislandelle (1994), « *La démarche de théorisation est difficile et périlleuse car il s'agit surtout de saisir la diversité et le contingent* ».

Selon Torrès (1998), ce courant de la diversité a pour conséquence une difficulté dans la généralisation des résultats, car soit il y'aura un aboutissement de plusieurs cadres d'analyse (approche typologique), soit un aboutissement d'une infinité de cas particuliers (approche contingente).

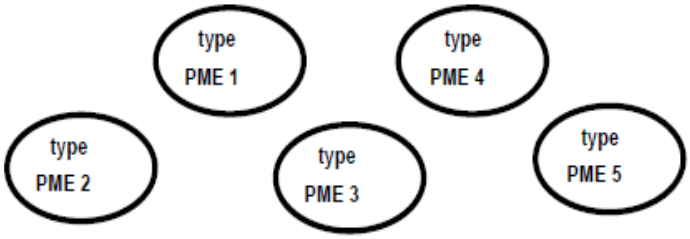


Figure 15 : Le courant de la diversité Torrès, (1998)

Nous nous sommes positionnés dans le courant de la spécificité de la PME, comme pour Torrès (1998), nous considérons que dans le domaine de la sécurité des SI, les études antérieures sont souvent menées dans des grandes organisations et sont peu ou pas du tout adaptées à la situation des PME car ces études n'ont pas tenu compte de leurs spécificités. Pour Torrès (1998), il devient très logique de s'intéresser aux PME, en se référant au paradigme de la spécificité des PME, dans l'objectif d'apporter un éclairage particulier à la sphère des PME sur un problème précis de gestion.

3.2. Caractéristiques des PME

Selon Mintzberg, (1998), le facteur de contingence le plus reconnu quant à ses effets sur la structure d'une organisation est la taille. Selon Brooksbank, (1991), avant de définir le concept de « petite entreprise », il convient de répondre à deux questions préalables : que signifie la taille et comment la mesure-t-on ? Où se situe la frontière critique entre les grandes et les petites entreprises ? Une classification présente dans la littérature proposée par Julien et Marchesnay, (1988 ; 1996), résumée dans le tableau suivant :

Taille (Effectif)	Description
1-9	Entreprises mono personnel, artisanales ou T.P.E.
10-19	Entreprises dont le statut ou le mode de gestion les apparente à des T.P.E.
20-50	Entreprises qui commencent à être structurées à la manière des moyennes entreprises.
51-200	Moyennes entreprises (la borne supérieure peut être augmentée à 500 selon les pays).

Tableau 10 : Typologie des entreprises (Julien et Marchesnay, 1988 ; 1996)

Et d'après l'INSEE[15], la catégorie des petites et moyennes entreprises (PME) est constituée des entreprises qui regroupent plus que 9 personnes et moins de 250 personnes (Décret n°2008-1354 Article 3).

La tranche d'entreprises qui va nous intéresser se situe donc entre 10 et 249 salariés et nous allons les regrouper en quatre catégories comme suit :

[10-19] : Petites entreprises dont le statut ou le mode de gestion les apparente à des T.P.E.

[20-49] : Entreprises qui commencent à être structurées à la manière des moyennes entreprises.

[50-99] : Moyennes entreprises

[100-249] : Moyennes entreprises qui commencent à être structurées à la manière des grandes entreprises.

Dans notre recherche, nous nous intéressons à la tranche d'entreprises qui se situe entre 10 et 250 salariés.

Passons maintenant aux spécificités de la structure et des fonctions occupées dans les PME comme cela est présenté dans la littérature. Pour Fourcade et Marchesnay, (1997), les PME ont des structures « plates », vu qu'il y a peu de niveaux hiérarchiques, et leur éventail de subordination, c'est-à-dire le nombre de personnes sous l'autorité du dirigeant, est plutôt développé. Ainsi, la direction est souvent assurée par un dirigeant, aidé parfois par un adjoint, ou encore deux associés. Dans ce sens, pour (Filion, 1991 ; Winston et Heiko, 1990 ; Julien et Marchesnay, 1988), dans le fonctionnement des PME, le propriétaire-dirigeant est un intervenant aussi important qu'omniprésent. De ce fait, et parce que la structure de la PME est souvent plus simple que celle de la grande entreprise, le propriétaire-dirigeant est susceptible d'être davantage en contact direct avec les fonctions opérationnels de son entreprise (approvisionnements, contrôle de la qualité, production etc.).

Sur le plan organisationnel, la PME est caractérisée par de petites unités de gestion plus autonomes, peu matures et dépendantes des expériences et de l'expertise du propriétaire-dirigeant (Winston et Heiko, 1990). Elle a un mode de fonctionnement basé sur une structure plus organique que hiérarchique ou mécaniste (Mintzberg, 1989). En conséquence, le processus

[15] Institut National de la Statistique et des Etudes Economique (INSEE) : https://www.insee.fr/fr/metadonnees/definition/c1565

de prise de décision est souvent peu complexe, axé sur l'action immédiate, et comporte un degré de formalisation moindre (d'Amboise, 1989 ; GREPME, 1994).

Tous ces éléments, montrent la grande importance du dirigeant dans le fonctionnement de la PME, ce qui va nous amener à développer le rôle joué par le dirigeant ultérieurement.

Fourcade et Marchesnay (1997), montrent que la formation au sein des PME est peu répandue car elle semble peu adaptée aux ses besoins : le manque de temps et de ressources, les problèmes d'organisation, font que souvent, les PME préfèrent la formation « sur le tas », et quand des formations sont mises en place, ce sont principalement des formations techniques, car « *les dirigeants veulent des résultats concrets face au sacrifice consenti* ». De plus, ils ont montré qu'il y a peu de supports d'information, car une entreprise de petite taille facilite la communication et accroît la proximité entre les personnels.

Ces deux derniers points, nous incitent à réfléchir vis-à-vis des possibilités de mise en place d'une démarche d'information et de formation liées à la sécurité des SI dans les PME.

3.3. La PME et le système d'information

La taille d'une entreprise peut également avoir des effets sur la stratégie informationnelle. De ce point de vue, il convient de mettre en évidence la valeur des réseaux développés par le dirigeant d'une PME : ils permettent d'obtenir à moindre coût une large part d'informations facilitant la consolidation de l'entreprise (Fourcade, 1991) et s'inscrivent dans un cheminement susceptible d'orienter le développement de l'entreprise au sein de son environnement immédiat (Pecqueur, 1989).

Les PME se préoccupent peu de la gestion des technologies de l'information (manque d'expérience ou de connaissances) et sous-utilisent leurs systèmes d'information par rapport aux plus grandes entreprises. Le lien entre l'utilisation des technologies de l'information et la taille des entreprises, s'explique généralement par les limites financières des entreprises de petite taille (Inman et Mehra, 1990 ; Golhar et al. 1990). Pour les PME, la proximité des clients et des dirigeants de l'organisation permet, en partie du moins, de suppléer aux lacunes du système d'information.

Plusieurs études ont notamment montré le rôle des SI dans la survie et le développement des PME (Levy, Powell et Yetton, 2002). Sharkas, (1974), indiquait que les faiblesses de PME

étaient majoritairement liées à des erreurs de décision de la part du dirigeant, en se focalisant sur le court terme, et le non-appui sur des SI performants.

Plus récemment, Perks, (2010), a montré que le système informatique et/ou les technologies de l'information et de la communication (TIC) peuvent être à l'origine de problèmes de croissance, en conséquence de leur inadaptation, ou de l'incapacité à fournir des informations favorisant la résolution de problèmes ou la prise de décision. Dans ce contexte, la PME doit être vigilante à la phase d'implantation, dont dépendront ensuite les modes d'utilisation par le dirigeant et les collaborateurs.

L'utilisation des SI est liée à la satisfaction des utilisateurs (Lees, 1987 ; Blackwell, Shehab et Kay, 2006). Raymond, (1985), a montré que les SI informatisés avaient une influence sur les décisions opérationnelles, mais pas sur les décisions stratégiques. Ceci est d'autant plus problématique pour les PME qui choisissent des progiciels intégrés, car l'investissement nécessaire pour leur acquisition est souvent très élevé comparativement à leurs ressources (Malone, 1985) et les outils sont souvent sous-utilisés (Dandrige et Levenburg, 2000).

Bidan, Rowe et Truex (2012) identifient trois types d'architecture des SI en PME, conduisant à différentes utilisations :

-Une architecture « en silos » : avec plusieurs bases de données non reliées, des politiques non formalisées, et des outils hétérogènes avec peu d'interfaces ;

-Une architecture partiellement standardisée avec un ERP partiel (nombre limité de modules installés) et d'autres logiciels en parallèle ;

-Une architecture mixte, avec des bases de données communes, un ERP largement utilisé, et des outils ad hoc.

Ces auteurs montrent que les entreprises les plus petites tendent à développer une architecture en « silos », dont les outils et les pratiques sont souvent bricolés.

Pour Jaouen et Nakara, (2014), l'implantation des SI et leurs modes d'utilisation sont contingents. En effet, le contexte organisationnel et stratégique influe fortement sur le type d'outil implanté et le type d'usage qui en sera fait (Gadille et D'Iribarne, 2000 ; Benghozi, 2001 ; Raymond, 2001 ; Mathrani et Viehland, 2009).

Pour certains auteurs, les PME n'ont généralement pas les moyens d'employer un personnel interne ayant une expertise en informatique (Noteboom, 1988; Spinellis et al. 1999). Cela

signifie que les PME sont confrontées à des risques et des problèmes concernant leur système d'information, pour Soh et al. (1992), les PME souffrent d'un manque de connaissances, disposent de matériels et de logiciels inadéquats, manquent de ressources financières et de support technique, ont des difficultés de recrutement, doivent compter sur des ressources externes, et ont des perspectives de management à court terme imposées par un environnement compétitif très mouvant.

Gupta et Hammond, (2005), reconnaissent les contraintes opérationnelles auxquelles doivent faire face les organisations comme : le manque de personnel ayant une expertise spécifique dans le domaine de la sécurité, le manque de compréhension ou l'inconscience vis-à-vis des risques, le manque de ressources financières pour faire appel à des consultants ou former le personnel et une incapacité à se focaliser sur la sécurité due à d'autres priorités d'affaires. Ces contraintes peuvent limiter leurs capacités à faire face aux problèmes de sécurité.

Pour Barlette (2006), pour qu'une sécurité satisfaisante existe, il est nécessaire de disposer d'un minimum : de technologies, afin d'assurer les protections de base (antivirus, firewall, sauvegardes, …); de procédures, telles les mises à jour, le suivi des sauvegardes, les contrôles et tests, et de compétences pour gérer ces technologies et les faire évoluer en adéquation avec la stratégie de l'entreprise. Alors, si les investissements en TIC ne sont pas en adéquation avec la stratégie de l'entreprise et que l'entreprise manque de solutions technologiques et de compétences, nous pouvons nous attendre à ce que la sécurité des informations des PME soit peu ou pas satisfaisante. Nous nous interrogeons, si ces contraintes peuvent intervenir sur le spectre des protections adoptées, les équipements technologiques, l'accompagnement et les formations destinées aux salariés et en général, sur la culture de sécurité des salariés et leurs comportements vis-à-vis de la sécurité des SI.

3.4. Les recherches sur la culture SSI dans les PME

Les chercheurs ont précédemment proposé divers cadres conceptuels pour la gestion de la SSI qui inclut le développement CSSI. Si ces cadres sont clairement utiles, ils représentent un champ théorique centré généralement sur les grandes organisations. En outre, ils ne traitent pas les défis de SSI rencontrés par les PME. Toutefois, quelques recherches se sont centrées sur l'étude de la culture sécurité dans les PME (Kuusisto et Ilvonen, 2003 ; Ngo et al, 2005 ;

Dojkovski et al, 2005, 2007 ; Williams, 2009 ; Kaur et Mustafa, 2013 ; Lopes et Oliveira, 2014 ; Santos-Olmo et al, 2016).

L'étude de Kuusisto et Ilvonen (2003) a été réalisée en Finlande, les données de leur étude ont été collectées à partir d'évaluations de la sécurité du SI effectuées dans 11 PME. Les PME évaluées agissent dans le domaine des entreprises à forte intensité d'information. Ainsi, leur activité dépend fortement de la technologie. Les évaluations ont été effectuées par des groupes d'étudiants dans le cadre du cours de gestion de la sécurité de l'Université de technologie de Tampere en Finlande.

Les évaluations ont été mises en œuvre sous forme d'entretiens semi-structurés basés sur des directives données aux étudiants. Une politique de sécurité du SI documentée n'a été trouvée que dans trois PME. Certaines PME possédaient des documents liés à des problèmes de SSI, mais il n'y avait pas de coordination de ces documents et ils n'avaient pas été collectés pour former une entité.

Les évaluations ont révélé une attitude alarmante; même une entreprise de 30 employés a déclaré qu'une politique de SSI documentée n'est pas nécessaire en raison de la petite taille de l'entreprise. En ce qui concerne la responsabilité de la SSI, l'arrangement le plus courant était que le responsable des systèmes d'information était responsable de la partie technique de la SSI. D'autres domaines de la SSI étaient soit pris en charge par cette personne également, soit, comme dans les grandes PME, c'était la responsabilité des cadres intermédiaires ou du responsable de l'information. De plus, presque personne n'avait vraiment documenté ses procédures de travail.

La plupart des entreprises ont admis que si une personne-clé était absente pendant une longue période, cela causerait des problèmes majeurs à leur entreprise. Même après avoir remarqué cela, les entreprises n'avaient pas commencé à documenter les tâches de travail clés. En général, aucune formation sur la SSI n'a été organisée dans les PME évaluées. La principale raison du manque de formation était le faible nombre d'employés et le peu de formations en général. Dans certaines PME, les problèmes de SSI étaient reconnus dans la formation d'un nouvel employé, et si une entreprise avait des procédures de SSI documentées, les documents étaient inclus dans le matériel de formation pour les nouveaux employés. Aucune formation régulière sur les problèmes de SSI n'a été organisée.

Après avoir évalué la situation de la sécurité des informations dans les PME étudiées, ces auteurs ont proposé des recommandations aux PME telles que :

- Les entreprises évaluées devraient commencer la documentation sur la SSI. En documentant une politique de SSI, ils peuvent commencer un processus de développement de la SSI en tant qu'entité. La documentation aurait les avantages suivants:

• Une compréhension unifiée des procédures de SSI

• Une formation plus facile pour les nouveaux employés

• Un outil d'amélioration de la SSI

• Instructions claires en situation de crise.

- Etablir des instructions documentées sur la manière dont les informations sont classées et donc traitées est nécessaire dans chaque PME. Le personnel doit être conscient que dans l'entreprise, il y a beaucoup d'informations qui devraient rester à l'intérieur de l'entreprise et qui ne devraient pas être stockées sur des ordinateurs de bureau où elles peuvent être consultées accidentellement ou intentionnellement par les visiteurs.

- En documentant un système de remplacement, l'entreprise peut s'assurer que les employés sont conscients de leurs responsabilités. La formation sur ce sujet permet de s'assurer que les gens prennent des mesures pour mettre à jour la documentation, et forment également indépendamment leurs remplaçants.

- La formation à la SSI n'a pas à être un cours magistral. Pendant les pauses-café partagées, lorsque des problèmes de SSI sont discutés, cela peut être comme une formation.

Ngo et al (2005), traitent le processus de transition (qui est l'ajustement, le développement et le changement que vivent les personnes au sein des organisations pour progresser vers la réalisation d'un changement particulier), pour le changement de la CSSI. Ils proposent également un modèle de transition décrivant les rôles des leaders et des suiveurs et leurs responsabilités respectives dans chacune des phases de transition. Le modèle était élaboré à partir de la recherche sur la CSSI et du cadre de processus de transition de Bridges (2003) qui peut être utilisé par les dirigeants et les employés des PME australiennes pour la transition vers un changement de CSSI.

L'étude de Dojkovski et al (2007), explore le sujet du développement d'une CSSI dans les PME et le contexte national dans lequel opèrent les PME. Ces auteurs ont mené une étude interprétative basée sur une revue de la littérature, deux groupes de discussion et trois études de cas dans des PME australiennes. Ensuite, ils ont proposé un cadre holistique pour favoriser une

CSSI dans les PME dans un cadre national. Cette recherche examine les principaux défis de gestion des PME qui tentent de développer une telle culture. Les principales conclusions suggèrent que les dirigeants de PME australiennes ne fournissent pas un soutien suffisant pour la SSI en raison d'une conscience insuffisante de son importance et peuvent être également affectés par les attitudes nationales face au risque. La recherche conclut que les dirigeants de PME australiennes peuvent bénéficier de l'adoption d'une approche de SSI fondée sur les risques et devraient être informés du rôle stratégique potentiel des technologies de l'information et de la SSI. Cette recherche identifie également la valeur et la difficulté de promouvoir une approche comportementale et un apprentissage de la SSI pour compléter les approches technologiques et managériales traditionnelles.

Leur cadre conceptuel holistique, décrit trois influences externes (culture nationale et éthique, initiatives gouvernementales et les fournisseurs de technologies) et des influences internes (leadership / gouvernance d'entreprise; la culture organisationnelle; la gestion; apprentissage individuel et organisationnel; sensibilisation à la sécurité organisationnelle; revoir / évaluer, comportementales). Les influences externes sont expliquées comme suit :

- **Culture nationale et éthique:** Les cultures nationales peuvent affecter la culture organisationnelle de la SSI et cette possibilité devrait être envisagée par les initiatives gouvernementales. De plus, les normes éthiques peuvent différer d'un pays à l'autre.

- **Initiatives gouvernementales:** Les gouvernements (fédéral et étatique) peuvent jouer un rôle de soutien clé, y compris, dans un contexte australien, la distribution de brochures de sensibilisation à la SSI aux PME et à la réalisation d'une analyse comparative nationale de la SSI des PME. Pour aider les organisations australiennes, des exemples de scénarios de risque de sécurité peuvent être développés à partir des ressources de sécurité des informations existantes.

- **Fournisseurs:** Les fournisseurs de technologies de SSI jouent un rôle clé. Ils peuvent fournir une sensibilisation à la SSI, mais ils peuvent également assurer la fiabilité des PME qui, autrement, pourraient sentir qu'on leur vent du matériel et des logiciels inutiles.

Quant aux influences internes, elles sont développées ci-dessous :

- **Leadership / Gouvernance d'entreprise:** Les dirigeants de PME doivent faire preuve de leadership dans l'organisation et agir en tant que modèle pour la SSI, prendre des initiatives

pour se renseigner sur la SSI et développer des structures de gouvernance d'entreprise pour fournir une assurance adéquate de la SSI.

- La culture organisationnelle : La culture organisationnelle locale affectera la CSSI. Par exemple, une culture ouverte favorise la désinvolture dans l'approche de la SSI.

-Gestion : Une plus grande sensibilisation et les résultats d'une analyse des risques étaient considérés comme essentiels pour garantir aux PME que des politiques et procédures formelles sont vraiment nécessaires. Deuxièmement, les PME devraient être guidées par les résultats d'un processus de protection contre la perte d'actifs pouvant découler d'une analyse des risques basée sur des scénarios provenant de contenus externes accessibles. Troisièmement, un budget devrait être alloué à la SSI, en particulier dans les PME où la fourniture de ressources appropriées peut facilement être négligée. Les PME seront aidées en évaluant régulièrement leur CSSI. Le contrat de travail, ou manuel de l'employé en l'absence de contrat, peut offrir des incitations et prévoir des sanctions concernant la conduite de SSI des employés, influençant ainsi la motivation des employés.

- Apprentissage individuel et organisationnel : L'apprentissage en ligne, la formation et l'éducation sont des initiatives potentiellement précieuses pour développer une CSSI pour les PME. Le partage des connaissances, la coopération et la collaboration ont été jugés importants pour l'apprentissage aux niveaux individuel et organisationnel afin de développer une CSSI.

- Sensibilisation à la sécurité organisationnelle : Le marketing de la SSI, en particulier, des mesures de sensibilisation informelles qui soutiennent la sensibilisation formelle fournie de l'extérieur sont essentielles. Des mesures de sensibilisation formelles et informelles ont déjà été suggérées pour les PME par Furnell et ses collègues (2004). Les mesures de sensibilisation doivent être convaincantes, comme le propose Siponen (2000).

-Examiner / évaluer: Les PME devraient régulièrement examiner et évaluer les mesures adoptées afin de s'améliorer continuellement.

-Comportementales: Une gamme d'initiatives externes et internes peut développer des traits comportementaux souhaitables de responsabilité, d'intégrité, de confiance et d'éthique.

Les principaux résultats de cette étude montrent que les dirigeants de PME australiennes ne comprennent pas suffisamment l'importance de la SSI pour leur entreprise. Ils ne comprennent pas également, la valeur stratégique des TI pour leurs entreprises. Une condition préalable au

développement d'une CSSI dans les PME est l'élaboration et la communication des politiques, procédures et responsabilités. L'étude a montré que la coopération, la collaboration, le partage des connaissances et l'apprentissage entre les employés de PME australiennes est une activité potentiellement intéressante. Enfin, dans un contexte national, l'étude met en évidence le défi majeur consistant à surmonter l'attitude de « laisser-faire » australienne à l'égard des problèmes de SSI.

Néanmoins, ce cadre est basé sur l'étude d'un petit groupe de PME australiennes et manque d'éléments spécifiques applicables uniquement aux PME (par opposition aux grandes entreprises). L'étude s'est concentrée sur l'enquête sur des PME techniques qui employaient du personnel qui ont des connaissances techniques. Cependant, ces entreprises manquaient de CSSI, ce qui permet de dire que les PME non techniques peuvent avoir des problèmes plus graves, suggérant un besoin de soutien externe plus fort. Enfin, le cadre est développé en concentrant uniquement dans le contexte de l'Australie et n'est donc pas valable pour les autres pays.

Williams, (2009), propose un modèle de la répartition des facteurs motivant et influençant la promotion de la culture de sécurité dans les PME. Il suggère que certains facteurs sont essentiels à la manière dont une culture de sécurité peut être facilitée et d'autres sont souhaitables. Les influences sur les pratiques de sécurité peuvent différer d'une organisation à l'autre et l'impact est différent d'une organisation à l'autre. En tant que tels, ils sont décrits comme discrétionnaires car certains peuvent exister et exercer une influence et d'autres pas. Les facteurs d'influence dépendront des communautés de pratique qui existent dans l'organisation. Le modèle vise à expliquer de nombreux facteurs qui posent des problèmes aux petites organisations dans la construction d'une CSSI. Parmi ces facteurs nous trouvons :

- Poussé par la réponse et non par la réaction (essentiel)
- Poussé par la responsabilité
- Influencé par la communauté de pratique (discrétionnaire)
- Influencé par la sensibilisation

Pour cet auteur, dans les petites organisations, les problèmes de la création d'une culture de sécurité comprennent: une réticence des organisations à investir dans des solutions non technologiques, c'est-à-dire la formation du personnel; un manque de contrôle sur les tiers ; ressources et expertise limitées et un manque de connaissances appropriées en matière de sécurité. Comme le rapportent Chia, Maynard et Ruighaver (2002), il est difficile de promouvoir une culture de la sécurité quand il y a un manque de gestion et de soutien financier pour améliorer la place de sécurité dans une organisation. Ce n'est pas nécessairement dû à un

manque de préoccupation mais plutôt à un manque de reconnaissance de l'importance de la sécurité et de ses conséquences. En outre, il ne fait guère de doute que les petites organisations sont fortement impactées par les systèmes d'information qu'elles utilisent et les contraintes auxquelles elles sont soumises sur le plan opérationnel. Cela crée plus de défis dans le maintien de la vie privée et de la confidentialité des informations dont elles sont responsables (Williams, 2009).

Kaur et Mustafa (2013), étudient la SSI dans une PME en Malaisie, du secteur de l'industrie aéronautique. En établissant la relation entre la connaissance, l'attitude, le comportement et la sensibilisation à la sécurité des informations. Un sondage par questionnaire a été utilisé pour collecter des données sur la sensibilisation à la SSI. Leur modèle est présenté dans la figure suivante, ainsi que leurs hypothèses de recherche :

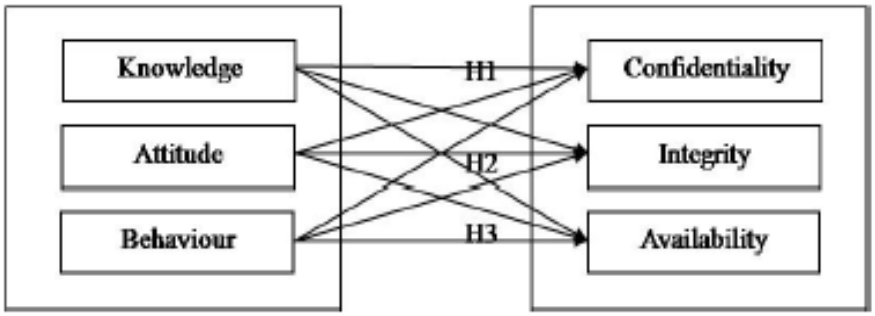


Figure 16 : Modèle de recherche de Kaur et Mustafa (2013)

Les principaux résultats indiquent qu'il y a relation entre l'attitude et le comportement des utilisateurs avec la sensibilisation à la SSI. La connaissance n'a montré aucune relation significative avec la sensibilisation à la SSI. Les résultats indiquent également que l'attitude et le comportement avaient une relation significative avec la confidentialité suggérant que les employés sont conscients de leurs responsabilités dans le maintien de la confidentialité des informations. Cette étude reste limitée à une seule organisation et les résultats ne peuvent pas être généralisés à d'autres PME.

Lopes et Oliveira, ont mené en 2014 une enquête sur la culture de la SSI dans les PME portugaises, 307 entreprises ont été interrogées : 100 sont des micro-entreprises (jusqu'à 9 travailleurs); 90 sont des petites entreprises (entre 10 et 49 travailleurs); et 117 sont moyennes. Parmi les 307 PME, 29 (9%) ont déclaré avoir une véritable CSSI et 278 (91%) ont adopté des mesures, mais celles-ci ne sont pas suffisamment pertinentes pour leur permettre de dire qu'elles ont une culture de sécurité. Les données montrent que les entreprises « moyennes » sont celles

qui possèdent le plus grand nombre de mesures de sécurité, suivies par les « petites » entreprises et les « micros » entreprises, se sont révélées être celles qui adoptaient le moins une CSSI. Cette étude fait la distinction entre les différentes tailles de PME et elle soutient l'idée que plus l'entreprise est grande en taille plus elle est susceptible d'avoir une meilleure SSI et une culture de sécurité positive.

Ces auteurs ont identifié des freins à l'adoption d'une CSSI, à savoir : la résistance et la désobéissance des utilisateurs. La résistance au changement est toujours élevée lorsque les routines de travail des utilisateurs sont modifiées, et l'adoption de mesures ne fait pas exception. Ainsi, la conversion de simples recommandations en actes normatifs obligatoires qui incluent l'adoption de restrictions pour ceux qui ne se conforment pas aux règles définies peut devenir un obstacle important à la mise en œuvre de mesures de SSI. Par conséquent, ces mesures devraient être complétées par un investissement important tant dans la promotion de l'importance du respect des règles de sécurité que dans la formation des utilisateurs.

Lopes et Oliveira (2014), selon leur enquête, ont identifié que le mécanisme de protection le plus couramment utilisé est le logiciel antivirus. Les pare-feux existent également en grand nombre, les filtres anti-spam et les sauvegardes sont également largement utilisés par les PME interrogées.

Plus récemment, Santos-Olmo et al, (2016), appartenant au GSyA Research Group, composé de professeurs de l'École d'informatique à l'Université de Castilla-La Mancha en Espagne, ont mené une étude en 2016, basée sur la méthode de la « Recherche-action ». Les bénéficiaires de cette méthode, ce sont toutes les PME qui souhaiteraient appliquer des méthodes avancées de gestion de la sécurité à leurs systèmes d'information afin d'améliorer la sécurité de leurs produits et processus informatiques dans un environnement contrôlé et de manière méthodique. Les résultats obtenus après la réalisation de cette recherche amélioreront l'efficacité des processus d'installation et de maintenance de la gestion de la SSI. Ensuite, ils ont analysé 12 travaux de recherche sur la culture de sécurité qui ont servi de base d'obtenir un ensemble de caractéristiques significatives pour la mise en œuvre du processus de la gestion de la SSI dans les PME. Une analyse comparative entre ces travaux de recherche a également été réalisée par ces chercheurs et une classification par groupes de caractéristiques a été faite et présentée ci-dessous :

Groupe 1. Caractéristiques orientées vers l'application des règlements-cadres

Normalisation: la mise en œuvre du processus sera basée sur la réglementation relative à la gestion de la SSI / Certification: ce processus permettra aux utilisateurs d'obtenir tout type de certification temporaire / Mesure: ce système permettra de mesurer le niveau de culture de sécurité de l'entreprise / Cultures: ce système prend non seulement en compte les aspects culturels internes, mais aussi la législation locale, sectorielle et internationale.

Groupe 2. Caractéristiques axées sur les aspects humains des utilisateurs

Adaptation progressive: le processus permettra d'adapter progressivement la culture de sécurité des utilisateurs / Approche théorique: le processus sera basé sur une approche théorique et réglementaire appropriée / Approche pratique: le processus sera orienté vers une application pratique vis-à-vis des utilisateurs / Aspects critiques: l'aspect humain sera considéré comme critique dans le processus de préparation / Facteurs psychologiques: les actions disciplinaires, clauses, récompenses pour les points, etc. et leurs effets sur la psychologie des utilisateurs lors de l'utilisation du processus seront pris en considération.

Groupe 3. Autres aspects souhaitables pour le processus

Orienté vers les PME: il doit avoir une orientation pour être valable aussi bien pour les grandes entreprises que pour les PME / Ressources à faible coût: il doit être orienté vers de faibles coûts en ce qui concerne la mise en œuvre et la maintenance du système / Cœur du SMSI (Système de management de la SSI): le processus de culture de sécurité est le processus principal du système de management de la sécurité de l'information (SMSI) / Base de connaissances dynamique: ce processus est capable d'apprendre des incidents de sécurité et de transformer ces faiblesses en forces en incorporant les incidents dans la base de connaissances afin de renforcer la culture de sécurité de ces aspects.

Malgré l'importance de ces travaux et cadres précédemment présentés, traitant de la CSSI dans les PME, leurs résultats ne peuvent pas être appliqués ou généralisés à toutes les PME à travers le monde, en raison de la spécificité culturelle de chaque pays, ce qui est de même pour les PME Françaises qui ont une culture d'entreprise spécifique par rapport aux autres pays comme les Etats Unis, le Japon ou les autres Etats membres de l'Union Européenne. Cela nous permet de poser la question suivante : Quel cadre peut être approprié dans le cas des PME Françaises et de la gestion de la CSSI ?

3.5. Le rôle clé du dirigeant de la PME dans la SSI

Rockwell (1968) affirme qu' « *un bon système d'information doit commencer au sommet par le directeur* ». Souvent, dans le cas des PME, le top management se résume au dirigeant, car la majorité des petites entreprises ont une structure organisationnelle plate et sont gérées par le propriétaire qui est souvent le directeur (Solomon, 1986). Autrement dit, les PME sont caractérisées par de petites unités de gestion plus autonomes, peu matures et dépendantes de l'expertise et des expériences du dirigeant (Winston et Heiko, 1990). Elles ont un mode de fonctionnement basé sur une structure plus organique que hiérarchique ou mécaniste (Mintzberg, 1989) et, ainsi, le processus de prise de décision est souvent peu complexe, axé sur l'action immédiate, et comporte un degré de formalisation moindre (d'Amboise, 1989 ; GREPME, 1994).

Pour Rockart et Crescenzi, (1984), sur le plan des SI, les dirigeants doivent vraiment « *réaliser que l'information est une ressource stratégique... Et ressentir de manière accrue le besoin d'être informés, motivés, et engagés dans les SI* ».

Selon Yap, (1989), deux raisons peuvent expliquer pourquoi la direction devrait apporter son soutien lors de l'évolution d'un système d'information : première raison est que la direction, avec sa vision plus globale, se trouve dans une meilleure position que les analystes pour identifier les opportunités d'affaires dans l'exploitation des technologies de l'information. La deuxième raison est que la mise en place d'un SI implique de très importants investissements et se trouve souvent liée à des implications s'étendant à l'ensemble de l'entreprise.

Archimbaud et Longeon, (1999), nous préviennent que « *la détermination et la supervision de la politique de sécurité sont des fonctions de direction. Rien de valable ne peut se faire sans le directeur* ». Le directeur joue donc un rôle très important, non seulement dans l'évolution du S.I. de son entreprise, mais aussi dans la mise en place d'une sécurisation qui puisse être satisfaisante. A ce sujet, Dutta et McCrohan, (2002), déclarent qu' « *adopter une position de sécurité implique un effort majeur de l'organisation, et la direction a un rôle significatif à jouer dans l'adoption de ces caractéristiques organisationnelles désirables.* ». Et pour Friend et Ridings Pagliari, (2000), « *quelle que soit l'organisation, la direction est fondamentalement responsable de la sécurité. Toute action lancée ou problème résolu devrait être une résultante de l'intervention de la direction* ». Pour Robinson et Volonino, (2004), le dirigeant serait le point de départ, en confirmant ceci : « *obtenir l'attention et l'implication du management afin*

de prendre en charge la gestion des risques organisationnels est la première étape de la prise en compte de la sécurité ».

Il a été démontré que les PME sont loin derrière les grandes entreprises dans la mise en œuvre de mesures de protection ou de contrôles de sécurité, car elles manquent de ressources financières et techniques (Cragg et al. 2011; Lábodi & Michelberger, 2010; Lee & Larsen, 2009). Premièrement, en raison de ce manque de ressources financières, il est difficile pour les PME de recruter et de retenir des spécialistes internes des TIC (Cragg et al. 2011; Kim et al. 2017; Pritchard, 2010). Deuxièmement, le dirigeant de la PME est souvent seul et n'a pas les compétences nécessaires pour identifier et mettre en œuvre des mesures d'atténuation des risques de sécurité des SI (Njenga & Jordaan, 2016). Souvent, ces PME font recours à une solution qui consiste à sous-traiter leur SSI à des sociétés externes ou à des consultants (Bhattacharya, 2011; Njenga & Jordaan, 2016). Le dirigeant de la PME peut également s'appuyer sur des solutions cloud pour leur sauvegarde ou sur un logiciel de sécurité SI basé sur SaaS[16] (Kim et al. 2017). Néanmoins, leur accès à des compétences externes est souvent limité par des ressources financières insuffisantes (Kim et al. 2017), et ces facilités d'externalisation traitent principalement des problèmes techniques mais ne traitent pas des problèmes socio-organisationnels du SSI comme la conformité des utilisateurs, qui est à ne pas négliger vu son importance dans l'augmentation de l'efficacité des mesures de sécurité non techniques (Barton et al. 2016).

Le dirigeant de la PME est le seul décideur dans la plupart des cas, et notamment en ce qui concerne les décisions stratégiques. Il joue un rôle central dans le choix et la mise en œuvre des mesures et contrôles liés à la SSI. Selon Njenga et Jordaan, (2016) le dirigeant de la PME n'est pas suffisamment conscient des problèmes de la SSI et considère la SSI comme une préoccupation des « grandes entreprises » (Rees, 2010). Pour (Mijnhardt et al. 2016), les cadres, les méthodes et les normes qui traitent la SSI tels que l'ISO 27002 sont également considérés par les dirigeants de PME comme trop complexes et comme étant principalement adaptés aux grandes entreprises, ce qui peut laisser le dirigeant sans références ou conseils appropriés.

Malgré l'importance des aspects stratégiques et financiers, ils ne doivent pas être les seuls à traiter, mais il faut aussi faire évoluer la PME en profondeur. Dans ce sens, Schein, (1990), affirme que le rôle du dirigeant est très important dans la mise en œuvre d'une culture et le

[16] Software as a service ou logiciel en tant que service, est un modèle d'exploitation commerciale des logiciels dans lequel ceux-ci sont installés sur des serveurs distants plutôt que sur la machine de l'utilisateur

changement de la culture. De plus, pour Fourcade et Marchesnay (1997), le dirigeant se conduit souvent en « père de famille » et a tendance à faire partager ses valeurs personnelles aux membres de son entreprise. Donc, plus la compatibilité entre les valeurs du dirigeant et celles des autres membres est élevée, plus la culture de la PME est forte. Hofstede et al. (1990), montrent que les valeurs des fondateurs et des dirigeants deviennent les pratiques des membres des organisations. Enfin, le soutien et l'implication de la direction transmettent des signaux forts dans toute l'organisation (Jarvenpaa et Ives, 1991; Grover, 1993).

De nombreux travaux scientifiques affirment que l'implication et la propension à agir des salariés sont directement dépendantes de celles du décideur (Forcht et Ayers, 2000; Barlette, 2005). Pour, Thong et Al., (1996), un soutien visible des dirigeants encourage les attitudes positives des utilisateurs face à l'utilisation des technologies de l'information. Les actions du dirigeant dans la sécurité des SI sont essentielles pour réduire les risques et garantir la conformité des employés à la SSI (Hu et al. 2012).

Tous ces arguments, nous laissent affirmer que le dirigeant de la PME joue un rôle clé dans l'assurance d'une meilleure sécurité des SI ainsi que la diffusion d'une culture de sécurité auprès des salariés. Sauf que ce rôle dépend du degré d'implication du dirigeant. Certains chercheurs ont montré que cette implication est influencée par le profil du dirigeant, tel que l'âge, le niveau d'éducation, et l'expérience dans une fonction donnée (Song, 1982), son ancienneté dans l'organisation (Helmich et Brown, 1972), son ancienneté dans la position hiérarchique (Stevens et al. 1978), en montrant que ces variables façonnent les attitudes et les perceptions des dirigeants au sujet des opportunités et des problèmes se présentant dans une entreprise.

Goodhue et Straub, (1991) ont réalisé une étude intéressante dans le domaine des risques liées aux SI, en étudiant les perceptions et l'implication des décideurs. Ils ont représenté cette implication à travers la figure suivante :

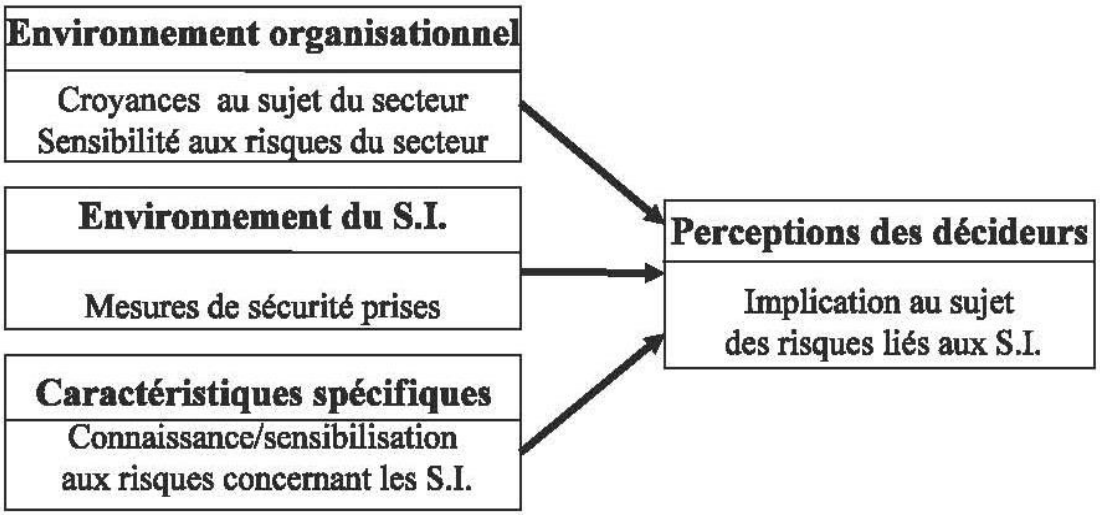


Figure 17 : L'implication au sujet des risques en S.I. Goodhue et Straub (1991)

Selon ce schéma, l'implication des décideurs dans la SSI de leurs organisations est fonction de trois grands facteurs qui sont les suivants :

- L'environnement organisationnel : risque inhérent au secteur, niveau de concurrence…

- L'environnement du SI : l'étendue des efforts consentis pour contrôler les risques liés aux SI (mesures de sécurité déjà prises).

- Caractéristiques spécifiques : telles que la connaissance de sinistres précédents, le niveau d'étude, l'expérience en SI…

Une étude de Barlette (2012), réalisée sur des PME, montre que les dirigeants peuvent adopter quatre types de comportements (Figure 18) :

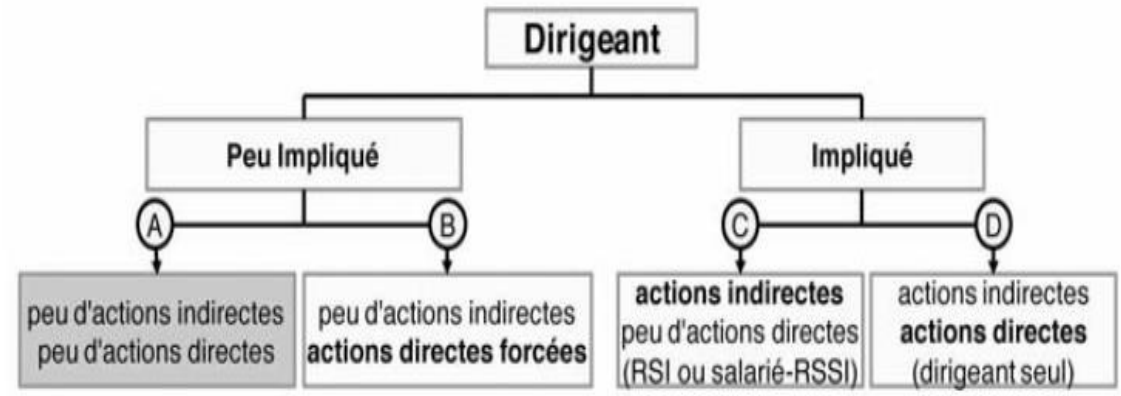


Figure 18 : Les actions directes et indirectes du dirigeant selon la situation (Barlette, 2012)

- La situation « A » correspond au cas d'un dirigeant qui n'est pas impliqué et n'agit pas, cette situation correspond à une SSI très faible,
- La situation « B » correspond au cas d'un dirigeant qui manque d'actions indirectes car il n'est pas impliqué, mais il effectuera certaines actions directes « forcées »,
- La situation « C » correspond à un niveau faible d'actions directes du dirigeant, qui sera compensé par une tierce personne (RSI ou salarié-RSSI),
-La situation « D » correspond à un dirigeant qui agit à la fois de manière directe et indirecte, les seules limites seront liées à l'échelle de ses priorités.

Une étude plus récente de Barlette et Jaouan (2019), qui porte sur les déterminants des comportements en SSI des dirigeants de PME, en distinguant les actions de protection des actions de soutien, montre que dans les plus petites PME, les dirigeants sont souvent seuls et obligés d'entreprendre des actions de protection. Cependant, si nécessaire, les dirigeants peuvent parfois compter sur d'autres personnels et donc adopter un comportement de soutien.

Nous avons montré l'importance du rôle du dirigeant de la PME dans la modification de la culture de sécurité de son entreprise à travers l'autorité qu'il dispose et à travers l'allocation des ressources nécessaires. Nous avons analysé également les variables et les facteurs qui peuvent influencer son implication ainsi que sa perception des risques. Certaines pistes permettent d'intervenir sur ces derniers, tels que les standards de sécurité de peuvent être utilisés pour gérer la sécurité et fournir les bases d'une approche cohérente de la sécurité des informations (Vermeulen et Von Solms, 2002; Bruce et Dempsey, 1997). Le dirigeant peut mettre en place les procédures et les règlements nécessaires. Selon Curvalle et Torrès, (1998), « *le dirigeant de la PME va jouer un rôle important, notamment dans la phase de lancement* (exemple: d'un processus de certification). *Il est le promoteur du changement de culture. Il doit notamment être en mesure d'expliquer pourquoi l'entreprise va recourir davantage aux procédures écrites* ».

Donc, ceci va permettre dans une certaine mesure de mieux sensibiliser les autres acteurs de la PME. Pour Monnoyer, (2003), dans la phase de sensibilisation des salariés aux TIC, non seulement le dirigeant de PME a un rôle à jouer, mais aussi interviendraient des variables plus contingentes telles que : des effets spécifiquement liés à la taille de l'entreprise.

Synthèse de la section 1

Tout au long de cette section, nous avons examiné la CSSI, en commençant par sa définition, la définition des concepts voisins comme la sécurité informatique et la sécurité des systèmes d'information. Ensuite, nous avons présenté l'état de l'art des travaux sur la culture sécurité (CS), les théories et les modèles concernant l'évaluation et la cultivation d'une CS, la gestion du changement de la CS. Nous avons présenté les instruments de mesure de la CS et la CS d'une vision économique. Nous avons montré la relation entre la culture organisationnelle et la culture sécurité. Par la suite, nous avons étudié la culture de sécurité des systèmes d'information (CSSI) dans les PME en passant par les caractéristiques de la PME, la place du système d'information dans la PME, les travaux sur la CS dans les PME et enfin le rôle clé du dirigeant de la PME dans la gestion de la sécurité du système d'information.

Section 2 : Les comportements liés à la sécurité

Dans le cadre de la compréhension des comportements des acteurs de l'organisation dans le domaine des systèmes d'information, plusieurs travaux ont utilisé des théories provenant des domaines : de la psychologie, de la criminologie, et ils ont étudié des aspects liés à l'éthique et la morale. Plusieurs modèles et théories sont apparus dans le cadre de l'acceptation et l'utilisation des technologies de l'information et ont été même mobilisés plus spécifiquement dans le domaine de la SSI. Dans cette section, nous nous présentons les modèles et théories qui permettent d'analyser les comportements liés à la sécurité. Ensuite nous allons analyser la relation entre la culture de sécurité et les comportements liés à la sécurité.

1. Les comportements dans le cadre de la SSI : Théories et modèles

1.1 Le modèle holistique de la SSI

Ce modèle a été bâti dans le cadre de la sécurité par J. et Y. Lee, (2002), qui ont lié la théorie de prévision du comportement avec les théories des liens sociaux, de l'apprentissage social et de la dissuasion, et ont donné naissance au modèle (Figure 19). Néanmoins, ce modèle n'a pas été validé sur le terrain, ce qui peut relativiser ses apports.

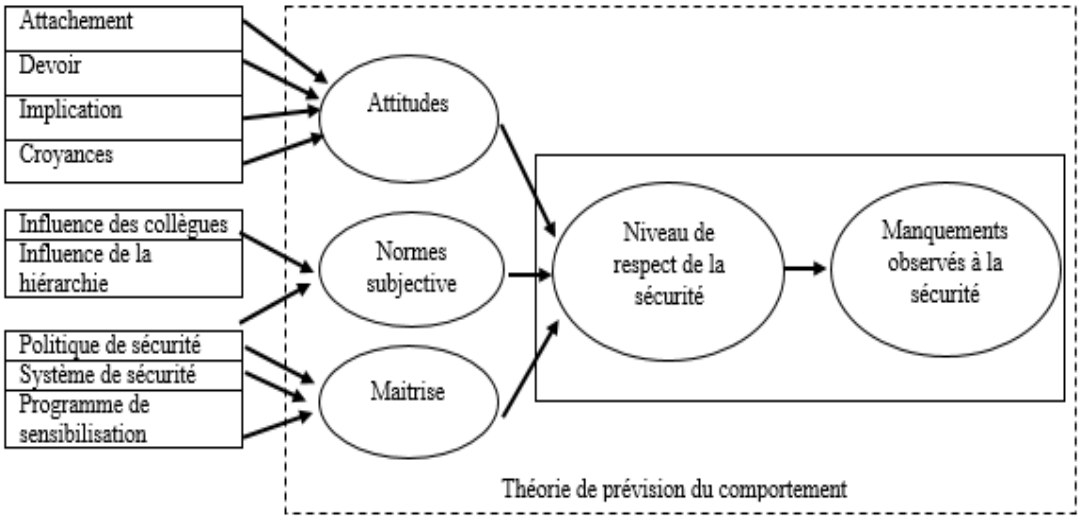


Figure 19 : Le "modèle holistique de la sécurité des informations" de J. et Y. Lee, (2002)

1.2 Les comportements liés à la sécurité

Selon Barlette (2005), les comportements sécuritaires sont classés **en comportements sécuritaires** « **positifs** », qui sont des comportements en conformité avec les règles de sécurité existantes dans l'entreprise, qu'elles soient écrites, contractuelles ou non, ou qu'elles soient verbales, et **en comportements sécuritaires** « **négatifs** », qui sont liés à un non-respect des règles, que ce soit un comportement lié à une perte de temps (par exemple, utilisation de l'Internet à des fins personnelles, ne pas signaler tout de suite un problème) ou un contournement des mesures de sécurité existantes.

Kraemer et Carayon, (2006), ont défini un cadre conceptuel des facteurs organisationnels et humains qui contribuent à la sécurité des "ordinateurs et des informations". Leur modèle est le suivant :

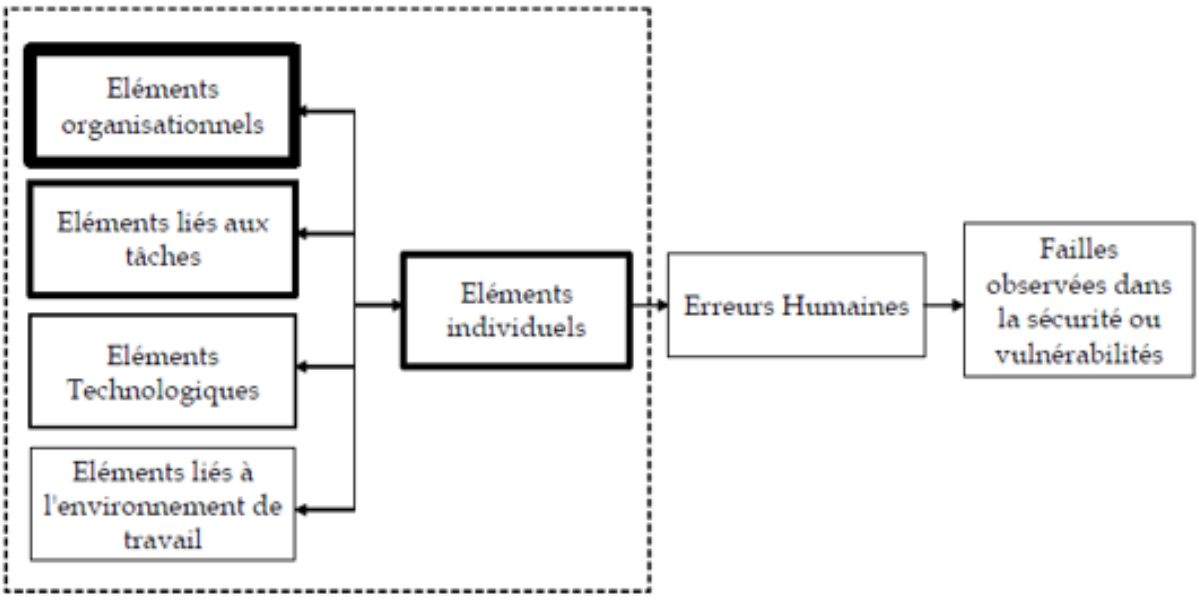


Figure 20 : Le cadre conceptuel "macro-ergonomique" de la sécurité des informations et des ordinateurs de Kraemer et Carayon, (2006) adapté de Barlette (2005)

Dans leur étude à travers des entretiens avec des administrateurs réseaux et des spécialistes de la sécurité, les éléments les plus représentés sont ceux liés à l'organisation (127 citations), puis à moindre titre ceux liés aux tâches (47 citations) et ceux liés à l'individu (36 citations), les éléments technologiques (22 citations), ceux liés à l'environnement de travail sont négligeables (4 citations). Les éléments relevés par les auteurs dans leur cadre conceptuel sont détaillés dans le tableau suivant :

Eléments	Thème	Définitions des auteurs	Citations
Organisationnels	**Culture sécuritaire**	Philosophie sécuritaire	37
	Structure organisationnelle	Organisation de la fonction "sécurité"	29
	Politique	Directives (ou manque de directives)	26
	Communication	Interactions entre les techniciens	24
	Autres		11
Liés aux tâches	**Charge de travail**	Temps libre laissé pour assurer la sécurité	23
	Devoirs	Appliquer les rustines, lancer l'antivirus	16
	Structure	Organisation des tâches ou des devoirs	8
Individuels	**Perception de l'utilisateur**	Incompréhension et manque de connaissances en sécurité de l'information	16
	Appréciation de la sécurité	Appréciation de l'état global de la sécurité	9
	Formation	Connaissances sécuritaires	8
	Autres		3
Technologiques	Logiciel, matériel inadéquat	Matériel/Logiciel qui ne peut être assez sécurisé : bugs, mots de passes, contrôles …	12
	Autres		10
Environnement de travail	Autres		4

Tableau 11 : Les principaux thèmes évoqués par Kraemer et Carayon, (2006)

Pour les éléments « organisationnels », le thème le plus cité est la « Culture sécuritaire » définie en tant que la philosophie sécuritaire avec 37 citations, ce qui rejoint notre préoccupation principale la culture sécurité dans le domaine de la sécurité des SI.

Une étude plus récente de Chen et Zahedi (2016), sur la sensibilité au contexte des perceptions et des comportements des utilisateurs en matière de sécurité en ligne aux attributs individuels, et sur les comportements des utilisateurs face à menaces de sécurité en ligne a vu le jour. Ces auteurs ont combiné la théorie de la motivation de protection (PMT) au comportement de sécurité en ligne avec une comparaison des comportements de sécurité des utilisateurs aux États-Unis et en Chine. Leur modèle conceptualisé est testé sur la base de 718 observations d'enquête recueillies aux États-Unis et en Chine. Leurs résultats montrent la divergence entre les États-Unis, un exemple de la société occidentale moderne, et la Chine, un exemple de la société orientale traditionnelle, dans la formation des perceptions de la menace. Leurs résultats ont également révélé les impacts modérateurs significatifs de la culture adoptée sur la façon dont les perceptions des menaces de sécurité et les évaluations d'adaptation influencent les comportements de sécurité et fournissent des informations sur les motivateurs et les modérateurs des comportements de sécurité en ligne des individus dans les deux pays.

1.3 Comportements liés à la sécurité en PME

Puisque les PME représentent un champ de recherche spécifique, nous allons présenter les recherches qui se sont intéressées aux comportements liés à la sécurité dans les PME.

Parmi les travaux qui ont cherché à comprendre les comportements liés à la sécurité des acteurs dans les PME, nous citons ceux d'Yves Barlette (2006) où il distingue les comportements des dirigeants, et les comportements des salariés à travers une étude réalisée au sein de huit PME Françaises. Les principaux résultats de son étude se résument ci-dessous :

- **Pour les comportements des dirigeants**

- Les principaux éléments qui vont limiter la marge de manœuvre des dirigeants sont le manque de temps et d'argent.

- Les entreprises dans lesquelles on trouve les dirigeants les moins impliqués n'ont pas forcément un niveau de sécurité faible car des mécanismes de compensation se mettent en place. Le principal mécanisme de compensation se manifeste par la prise en charge de la gestion de la sécurité du S.I. par un salarié qui va assumer en plus de sa charge le rôle d'un RSI.

- Le niveau de sécurité dans les entreprises dans lesquelles les dirigeants délèguent la responsabilité de la sécurité est dans la majorité des cas sensiblement plus faible que dans celles où le dirigeant conserve son rôle de gestion de la sécurité.

- **Pour les comportements des salariés**

- Les caractéristiques personnelles sont le principal moteur des comportements liés à la sécurité dans les PME. Les six facteurs les plus importants étaient les motivations personnelles, la préservation de l'intimité, les motivations liées au poste, les motivations liées à l'entreprise, l'habitude et le vécu.

- Les limitations des comportements liés à la sécurité des salariés sont principalement liées au manque de temps, autrement dit à l'équilibre entre le temps de travail et le temps qui peut être affecté aux comportements liés à la sécurité. Les limitations sont aussi liées à un manque d'information, de sensibilisation et de formation, ce qui peut être dû à des problèmes de temps disponible, et plus globalement un problème de ressources financières.

Il propose un modèle ou un cadre d'analyse des comportements liés à la sécurité. Pour les facteurs environnementaux, nous trouvons : le secteur, la concurrence, etc. le prestataire extérieur ce sont les actions, mises en place par le prestataire extérieur que ce soit au niveau technique, procédural ou organisationnel. Il représente aussi les échanges entre les différents acteurs : dirigeant, RSI, salariés et prestataire extérieur. Pour P1, P2, P3 et P4 représentent les quatre propositions de recherche où P1 et P2 concernent le dirigeant, P3 et P4 concernent les salariés. Les principaux résultats de ces propositions sont présentés dans la figure 21 :

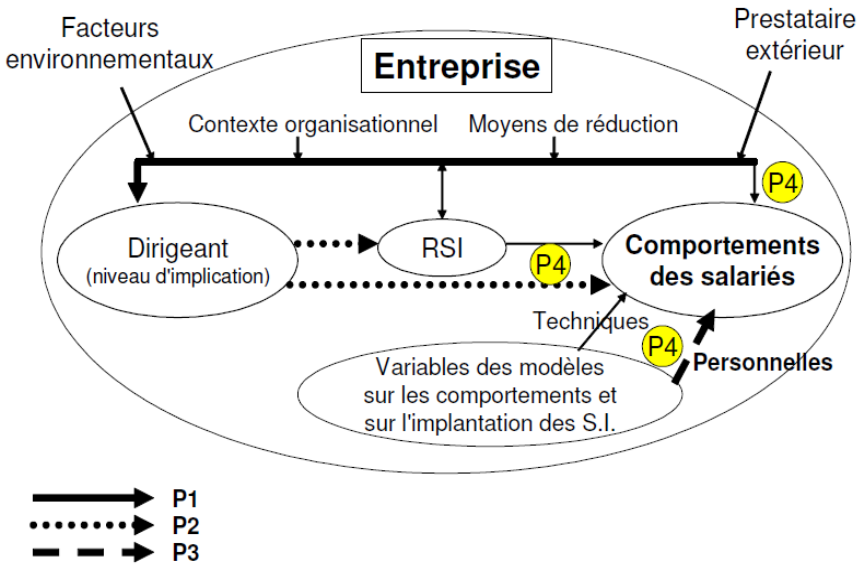


Figure 21 : Ethologie de la sécurité des S.I. : les facteurs (Barlette, 2006)

Cette recherche comprend les limites usuelles liées à la méthodologie qualitative adoptée qui peut poser un problème de généralisation des résultats, du fait de conclusions basées sur huit cas uniquement.

Une étude de Lee et Larsen (2009) à travers une enquête empirique sur les facteurs affectant la décision des dirigeants des PME d'adopter un logiciel anti-malwares[17] pour leur organisation. Un modèle de recherche a été développé en appliquant la théorie de la motivation de protection de la psychologie de la santé, qui a été utilisée avec succès pour étudier l'effet de la menace et de l'évaluation d'adaptation sur les actions de protection. Une enquête de terrain basée sur un questionnaire auprès de 239 dirigeants de PME américaines a été menée et les données ont été analysées à l'aide des moindres carrés partiels (PLS). Les principaux résultats de cette étude

[17] Un logiciel anti-malwares est un logiciel qui détecte et supprime les logiciels malveillants

montrent que l'évaluation des menaces et de l'adaptation permet de prédire avec succès l'intention d'adoption des logiciels anti-malware par les dirigeants des PME. En outre, l'influence sociale des principales parties prenantes et des variables spécifiques à la situation, telles que le budget informatique et le soutien des fournisseurs, tient compte des écarts considérables dans l'intention d'adoption et l'adoption réelle au sein des PME.
Cette étude n'a pas examiné l'impulsion des variables PMT, en supposant que les sujets sont pleinement conscients de la menace d'attaques de logiciels malveillants et de l'efficacité des logiciels anti-malware pour la contrer. Des expériences contrôlées sont recommandées pour mieux comprendre l'influence des différents types d'impulsions. Enfin, cette étude, n'a pas examiné les effets des variables qui caractérisent les PME, y compris le secteur d'activité.

Une étude de Barlette et al (2017), présente une recherche basée sur la théorie de la motivation à la protection (PMT) qui cherche à répondre à la question traite de la question : quels facteurs peuvent expliquer les comportements relatifs à la protection des informations des dirigeants de PME ? Ils ont mené une étude auprès de 292 dirigeants de PME, les données collectées ont été analysées à travers la méthode des moindres carrés partiels (PLS). Ils ont testé l'influence de la PMT sur deux sous-populations : les dirigeants propriétaires (n=183) et non-propriétaires (n=109). Leurs résultats mettent en lumière des différences importantes et significatives entre ces deux sous-groupes. L'originalité de notre travail tient au fait qu'il constitue la première étude dédiée aux comportements des dirigeants de PME en matière de protection des informations, distinguant de plus les propriétaires des non-propriétaires. Notre principale contribution théorique correspond à la mise en évidence et à l'étude de cette population différenciée, à approfondir dans de futures recherches. Les facteurs qui sont à la base des comportements de protection des dirigeants-propriétaires sont presque en contraste, comparés à ceux des dirigeants non-propriétaires.

Les résultats pour les non-propriétaires confirment et prolongent les recherches sur la théorie de motivation de protection en se concentrant sur une population qui n'avait pas encore été spécifiquement étudiée. À l'inverse, les résultats pour les propriétaires de PME ont été significativement différents et ont mis en évidence la nécessité de considérer des variables supplémentaires, telles que l'impact de l'influence sociale, ce qui confirme qu'il existe d'autres variables autres que les variables de PMT pourraient influencer leurs comportements.

Une étude plus récente de Barlette et Jaouan (2019), qui porte sur les déterminants des comportements en SSI des dirigeants de PME, en distinguant les actions de protection des actions de soutien. Cette étude montre que dans les plus petites PME, les dirigeants sont souvent seuls et obligés d'entreprendre des actions de protection. Cependant, si nécessaire, les dirigeants peuvent parfois compter sur d'autres personnels et donc adopter un comportement de soutien.

2. Relation entre culture sécurité et comportements liés à la sécurité

Dans cette partie, notre objectif est d'examiner les recherches qui traitent la relation entre la culture sécurité et les comportements liés à la sécurité dans le domaine des SI.

D'Arcy et Greene (2009), examinent la relation entre la culture de sécurité et les comportements des utilisateurs: la conformité à la politique de sécurité et le comportement de rôle supplémentaire de sécurité. Les données d'enquête ont été recueillies à partir de 105 ordinateurs à l'aide de professionnels dans des organisations situées aux États-Unis. Les résultats fournissent des preuves solides que la culture de sécurité contribue à un comportement des utilisateurs conforme. Peut-être encore plus intéressant, les résultats suggèrent une forte association entre la culture de la sécurité et des comportements de sécurité plus proactifs tels que la participation à une formation volontaire sur la sécurité et la promotion de pratiques de sécurité auprès des collègues.

Une autre étude de ces mêmes auteurs réalisée en 2014, qui examine l'influence des facteurs liés à la sécurité et aux relations de travail sur les décisions des employés en matière de conformité à la sécurité, et ils ont montré que la culture de la sécurité, la satisfaction au travail et le soutien organisationnel perçu ont un effet positif sur les intentions de conformité des employés en matière de sécurité.

Alfawaz et al (2010), présentent un cadre conceptuel sur la base des preuves issues de trois études de cas exploratoires pour classer et organiser les caractéristiques des sujets organisationnels impliqués dans des pratiques de SSI, en identifiant les comportements liés à quatre modes de pratique de la SSI. Leur cadre élargit les perspectives traditionnelles du comportement humain et de l'environnement social en identifiant comment les connaissances, les compétences et les préférences individuelles agissent pour influencer les pratiques

individuelles et de groupe en matière de gestion de la SSI. Leurs résultats montrent que l'ensemble de croyances ou de culture personnelle d'une personne joue un rôle majeur dans l'influence de son attitude personnelle à l'égard de son comportement de sécurité. Par conséquent, la compréhension de leurs croyances sous-jacentes est cruciale dans le processus de changement de comportement. Ils montrent aussi l'influence de la technologie, de l'environnement social, de la réglementation et de l'intérêt personnel qui contribuent aux comportements liés à la sécurité des employés. En conséquence, les membres d'une organisation peuvent manifester des comportements de différents modes à différents moments dans le temps. Ce mouvement continu rend difficile la sécurisation du système d'information d'une organisation en adoptant un seul mode de manière isolée. Par conséquent, il faut des efforts en jouant sur ces facteurs pour améliorer les comportements liés à la sécurité et les ramener à un mode optimal homogène.

Dans le même sens, une étude de Parsons et al (2015), présente trois aspects de la prise de décision en matière de SSI à savoir, la connaissance des politiques et des procédures, l'attitude à l'égard des politiques et des procédures et le comportement autodéclaré qui ont été examinés en conjonction avec les facteurs organisationnels susceptibles d'augmenter les cyber-vulnérabilités humaines. Leurs résultats d'une enquête menée auprès de 500 employés australiens ont révélé une relation positive significative entre la prise de décision en matière de SSI et la CSSI. Cela suggère que l'amélioration de la culture de sécurité d'une organisation influencera positivement le comportement des employés, qui à son tour devrait également améliorer le respect des politiques de sécurité. Cela signifie que le risque pour les SI et les données d'une organisation sera atténué.

Dans une autre logique, nous trouvons l'étude de Da Veiga et Eloff (2010), L'interaction entre les composants de SSI (comme la politique de sécurité, management de la sécurité etc.) et le comportement des employés a un impact sur la CSSI. Et elles proposent le cadre d'analyse suivant :

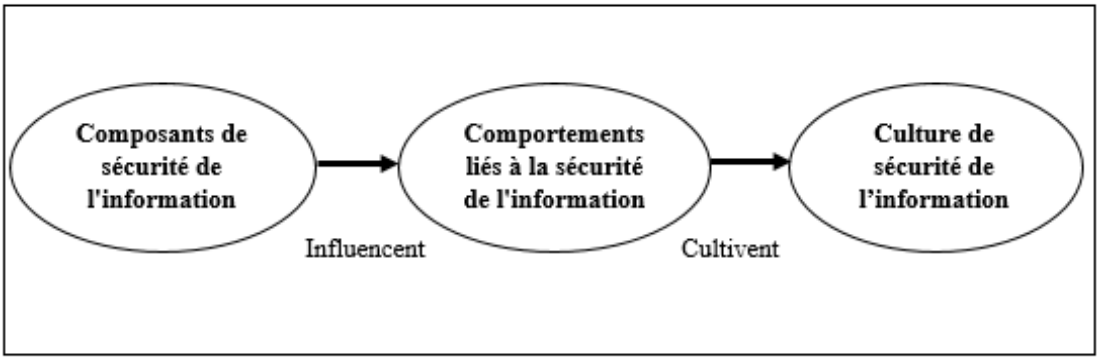


Figure 22 : Influencer le comportement de sécurité de l'information et cultiver une culture de sécurité de l'information (Da Veiga et Eloff, 2010)

Pour elles, la mise en œuvre des composants de sécurité tels que la politique de sécurité, programmes de sécurité, leadership etc. impacte l'interaction des employés avec les actifs informationnels, et par conséquent les employés présentent certains comportements appelés « Comportements de SSI ». Ces comportements peuvent se manifester dans la déclaration des incidents de sécurité, le respect de la politique de sécurité ou la protection des documents confidentiels. Avec le temps, ces comportements de sécurité évoluent au fur et à mesure que les choses se font dans l'organisation et donnent naissance ou cultivent une CSSI. Une culture est ainsi promue dans laquelle la SSI est acceptée comme la façon dont les choses sont faites dans l'organisation.

Le tableau suivant résume les travaux qui traitent la relation entre la culture de sécurité et les comportements liés à la sécurité :

Auteur	**Déterminants/ influence culture sécurité**	**Déterminants comportements de sécurité**	**Résultats**
D'Arcy et Greene (2009)	-Engagement de la direction -Communication de sécurité -Surveillance informatique	-La conformité à la politique de sécurité -Le comportement de rôle supplémentaire de sécurité	Forte association entre la culture de la sécurité et des comportements de sécurité plus proactifs tels que la participation à une formation volontaire sur la sécurité et la promotion de pratiques de sécurité auprès des collègues.

Alfawaz et al (2010)	-Les connaissances, -Les compétences -Les préférences individuelles	-Les pratiques individuelles et de groupe en matière de sécurité	-L'ensemble de croyances ou de culture personnelle d'une personne joue un rôle majeur dans l'influence de son attitude personnelle à l'égard de son comportement de sécurité. - La technologie, de l'environnement social, de la réglementation et de l'intérêt personnel qui contribuent aux comportements liés à la sécurité des employés.
Da Veiga et Eloff (2010)	-Hypothèses de base -Valeurs -Artefacts et créations	-Niveau organisationnel -Niveau de groupe -Niveau individuel	Les comportements liés à la sécurité des employés cultivent une CSSI.
D'Arcy et Greene (2014)	-Engagement de la direction -Communication de sécurité - Surveillance informatique	-Intention de conformité à la sécurité	-La culture de la sécurité, la satisfaction au travail et le soutien organisationnel perçu ont un effet positif sur les intentions de conformité des employés en matière de sécurité.
Parsons et al (2015),	-Sanctions et récompenses -Le rôle professionnel de l'individu -Le nombre d'employés dans l'organisation.	-La connaissance des politiques et des procédures, -L'attitude à l'égard des politiques et des procédures -Le comportement autodéclaré	Les employés avec une meilleure CSSI étaient plus susceptibles d'avoir des connaissances, attitudes et comportements conformes aux politique et procédures de SSI.

Tableau 12 : Les travaux traitant la relation entre la culture sécurité les comportements liés à la sécurité

Malgré le nombre intéressant de travaux qui traitent la relation entre CSSI et les comportements liés à la sécurité, nous constatons un manque de lignes directrices qui pourraient être utilisées pour établir efficacement une CSSI dans l'amélioration du comportement de sécurité dans les organisations. La plupart des études ne se sont pas concentrées sur l'examen de la relation entre le CSSI et le comportement de sécurité, peu d'études empiriques qui ont examiné cette relation ne pouvaient pas non plus fournir suffisamment de preuves empiriques sur l'effet réel de la CSSI sur le comportement de sécurité ou inversement. Cela était dû aux approches adoptées en termes de conceptualisation et d'opérationnalisation de la CSSI ainsi qu'au manque d'intégration avec le cadre comportemental théorique. Par conséquent, la conceptualisation de la CSSI en tant que concept multidimensionnel et l'adoption de la théorie comportementale devraient être envisagées et incorporées pour ce type d'étude. Il produira des résultats plus ciblés et complets sur la relation qui à leur tour pourraient être utilisés comme stratégies efficaces de CSSI pour améliorer le comportement de sécurité des employés dans les organisations.

Synthèse de la section 2

Nous avons consacré cette section à l'étude des comportements liés à la sécurité, en examinant en premier lieu les théories et modèles des comportements : les théories comportementalistes, les modèles de l'acceptation de la technologie et de l'ordinateur, modèles de la psychologie et de la criminologie et les aspects liés à la morale et à l'éthique. En deuxième lieu, nous avons présenté les modèles et théories traitant les comportements dans le cadre de la sécurité des informations et des SI : le modèle holistique de la sécurité des informations, les comportements liés à la sécurité et les comportements liés à la sécurité dans le cadre des PME.
Et en fin de cette section, nous avons examiné les travaux qui ont étudié la relation entre la culture sécurité et les comportements liés à la sécurité.

Section 3 : Les actions à mettre en place pour sécuriser les systèmes d'information

Nous allons dans un premier temps présenter ce que sont les notions de menace, risque, vulnérabilité et sinistre. Dans un deuxième temps, nous allons faire le tour des mesures de sécurité qui peuvent diminuer ou éliminer les notions précédemment citées et nous insisterons surtout sur l'importance de la sensibilisation et de la formation.

1. Menaces, risques, vulnérabilités et sinistres

Guinier, (1992), définit une **menace** comme un « *danger que peuvent faire peser des phénomènes naturels ou humains, volontaires ou non et dont la réalisation conduit à des sinistres. Elle peut être active ou passive ».*

Selon Pipkin, (2000), les menaces peuvent être délibérés ou fortuites, internes ou externes. Pour illustrer le propos de Pipkin, Barlette (2005) a effectué une classification à deux niveaux des menaces (Tableau 13) :

Provenance	Cause	Type	Exemples
Interne	Délibérée	Logiciel malveillant	Virus, logiciel d'attaque
		Actes de Malveillance	Destruction logique ou physique, vol
	Fortuite	Erreur humaine	Effacement accidentel, pas de sauvegarde
		Pannes matérielles, logicielles	Panne d'alimentation ou disque, blocage de logiciel
Externe	Délibérée	Actes de Malveillance	Piratage, Vol, atteinte à l'image
	Fortuite	Pannes d'infrastructure	électricité, télécommunications
		Evènements naturels	Inondations, ouragans, tremblement de terre
		Dommages collatéraux	Extension de l'attaque d'un partenaire (pirate ou virus)

Tableau 13 : Classification à deux niveaux des menaces (Barlette, 2005)

Pour, Brodeur (2006) le concept de **risque** occupe une place grandissante dans les travaux sur la sécurité. Pour lui, un risque constitue un danger dont on peut tenter d'estimer la probabilité qu'il s'actualise. Sheptycki (2004) reprend une distinction entre le risque (*risk*) et la menace (*threat*), initialement formulée par des chercheurs belges (Black et al. 2000). Dans cette perspective, le risque est le degré de probabilité qu'un dommage soit infligé et la menace est une estimation des capacités et du degré de motivation de la source humaine d'un risque.

Quant à la vulnérabilité, elle vient du latin Vulnus et vulnerare qui veut dire blesser, endommager, porter atteinte à, faire mal à, froisser, offenser (Lardeux, 2014 ; Absil, 2014 ; Bellier et al. 2002). De ce qui précède, La vulnérabilité peut être définie comme étant le caractère de ce qui est vulnérable, donc de ce qui est fragile ou précaire et peut être blessé, attaqué, endommagé (Absil, 2014, Mara, 2010). Absil (2014) précise en disant que la vulnérabilité est en général une possibilité, voire une probabilité, d'être affecté, blessé par des éléments internes ou externes.

Pour Gonik, (1996), la vulnérabilité « *caractérise différents niveaux de faiblesse de l'entreprise (…) par rapport aux menaces et aux risques qu'elles font naître. Être vulnérable, c'est être dans un état tel que l'on est susceptible de subir une atteinte. La vulnérabilité apparaît par l'existence simultanée d'un risque (et donc de la menace qui l'a fait naître), et d'une faiblesse* ».

Pipkin, (2000), introduit en plus la notion de procédures : « *La vulnérabilité correspond à une condition, une faiblesse, une absence de procédures de sécurité et de contrôles qui peuvent être exploitées par une menace* ».

Ces notions de procédure et de contrôle sont importantes, car si on ne met pas en place des procédures de sécurité ou si on ne teste pas ces procédures de sécurité, cela peut causer des vulnérabilités importantes. À travers le tableau suivant, nous présentons les types de vulnérabilités classées en vulnérabilités « classiques » ou conventionnelles et les « nouvelles » vulnérabilités apparues ces dernières années, qui résultent de plusieurs évolutions.

Type	**Exemples vulnérabilités « classiques »**	**Exemples de « nouvelles » vulnérabilités**
Matériel	Balayage écran, BIOS	Médias portables (clés USB);
Logiciel	Conception, Tests (failles), mise à jour insuffisante, utilisation détournée, vulnérabilités connues des pirates.	Open source; Equipes de programmation distantes;
Infrastructure	EDF, réseaux, télécoms, …	Téléphonie sur IP, réseaux sans fil; Ouverture des réseaux (vers partenaires, accès distants, extranet, e-commerce);
Processus de contrôle	Règles mal mises en place, mal interprétées, contournées, insuffisamment à jour	Mauvaise intégration des nouvelles technologies et habitudes;
Employés	action psychologique	Développement du nomadisme, de l'externalisation;
Serveurs	Mauvaise gestion des droits d'accès, administration des erreurs etc.	Virtualisation.

Tableau 14 : Les types de vulnérabilités et leurs sources (Adapté de Barlette, 2005)

Parmi les vulnérabilités les plus connues de nos jours, nous citons :

Vulnérabilité	Définition
Shellshock ou« Bashdoor »	est une vulnérabilité qui impacte les systèmes Linux, Unix et macOS. Elle autorise un attaquant à prendre le contrôle d'une machine.
Heartbleed	permet à un attaquant de lire des portions de mémoire d'un serveur, principalement des clés privées utilisées dans le chiffrement des communications ou d'autres secrets d'un serveur.
Poodle pour Padding Oracle on Downgraded Legacy Encryption	localisée dans un protocole de chiffrement, le SSLv3, cette faille rend les applications vulnérables aux attaques.
Dirty COW (COW pour « copy-on-write »)	est une vulnérabilité de Linux. Son exploitation peut permettre une élévation de privilèges.
Spectre et Meltdown	sont des vulnérabilités touchant les processeurs, principalement ceux de la société Intel pour récupérer des informations de la mémoire.

Tableau 15 : Exemples de vulnérabilités les plus connues
(Source : Orange Cyberdéfense, 2019)

Et enfin, pour le **sinistre** selon Guinier, (1992), il correspond à « *la réalisation d'un risque* ». Donc, si nous parlons d'un sinistre, nous sommes face à un problème, et il faut l'identifier rapidement afin d'en limiter les impacts.

Nous allons développer dans les titres suivants, quelles sont les mesures qui permettent de limiter les vulnérabilités et les menaces et ainsi de limiter les probabilités de la concrétisation des risques en sinistres. Nous avons distingué les mesures de sécurité en mesures techniques, mesures organisationnelles et mesures humaines.

2. Les actions techniques

Cette partie concerne les mesures techniques de sécurité, ça veut dire les mesures liées à la partie technique du système d'information : logiciels, matériels, serveurs, infrastructures etc. En effet, la sécurité des SI a ceci de caractéristique qu'elle est en perpétuelle évolution. Vu le développement technologique rapide, plusieurs vulnérabilités et menaces apparaissent et en parallèle, des mesures et des moyens mobilisées pour contrer ces menaces et ces vulnérabilités

évoluent. Donc, nous allons faire le tour des mesures que nous estimons les plus essentielles pour sécuriser l'organisation.

Selon un guide publié par La Cnil (Commission nationale de l'informatique et des libertés) rappelant les précautions élémentaires à mettre en œuvre pour aider les professionnels dans la mise en conformité à la loi Informatique et Libertés et au règlement général sur la protection des données. 17 mesures de sécurité ont été proposées dans ce guide, nous allons citer parmi lesquelles les mesures techniques :

Mesure	**Explication**	**Exemple d'outils/ précautions**
Authentifier les utilisateurs	Pour assurer qu'un utilisateur accède uniquement aux données dont il a besoin, il doit être doté d'un identifiant qui lui est propre et doit s'authentifier avant toute utilisation des moyens informatiques.	Contrôle d'accès logique.
Tracer les accès et gérer les incidents	Tracer les accès et prévoir des procédures pour gérer les incidents afin de pouvoir réagir en cas de violation de données (atteinte à la confidentialité, l'intégrité ou la disponibilité).	Dispositif de gestion des traces et des incidents.
Sécuriser les postes de travail	Prévenir les accès frauduleux, l'exécution de virus ou la prise de contrôle à distance, notamment via Internet.	Pare-feu, antivirus, mise à jour régulière des logiciels et antivirus, limiter la connexion de supports mobiles (clés USB, disques durs externes, etc.)
Sécuriser l'informatique mobile	Anticiper l'atteinte à la sécurité des données consécutive au vol ou à la perte d'un équipement mobile.	Cryptographie : Prévoir des moyens de chiffrement des postes nomades et supports de stockage mobiles.
Protéger le réseau informatique interne	Autoriser uniquement les fonctions réseau nécessaires aux traitements mis en place.	-Limiter les accès Internet, -Gérer les réseaux Wi-Fi. Ils doivent utiliser un chiffrement à l'état de l'art (WPA2 ou WPA2-PSK avec un mot de passe complexe) et les réseaux ouverts aux invités doivent être séparés du réseau interne. - Imposer un VPN[18] pour l'accès à distance.

[18] Un réseau privé virtuel, est un système permettant de créer un lien direct entre des ordinateurs distants, qui isole leurs échanges du reste du trafic se déroulant sur des réseaux publics.

		- Des systèmes de détection d'intrusion (IDS) peuvent analyser le trafic réseau pour détecter des attaques.
Sécuriser les serveurs	Renforcer les mesures de sécurité appliquées aux serveurs.	-Adopter une politique spécifique de mots de passe pour les administrateurs - Installer les mises à jour critiques - Mettre en œuvre le protocole TLS (en remplacement de SSL), ou un protocole assurant le chiffrement et l'authentification pour tout échange de données sur internet.
Sécuriser les sites web	S'assurer que les bonnes pratiques minimales sont appliquées aux sites web.	- Mettre en œuvre le protocol TLS (en remplacement de SSL) sur tous les sites web - Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées - Si des cookies non nécessaires au service sont utilisés, recueillir le consentement de l'internaute après information de celui-ci et avant le dépôt du cookie - Limiter le nombre de composants mis en œuvre, en effectuer une veille et les mettre à jour.
Sauvegarder et prévoir la continuité d'activité	Effectuer des sauvegardes régulières pour limiter l'impact d'une disparition non désirée de données.	- Effectuer des sauvegardes fréquentes des données, - Stocker les sauvegardes sur un site extérieur - Rédiger un plan de reprise et de continuité d'activité informatique (PRA[19], PCA[20]) - Prévoir une redondance matérielle des matériels de stockage.
Chiffrer, garantir l'intégrité ou signer	Assurer l'intégrité, la confidentialité et l'authenticité d'une information.	- Les signatures numériques, - Le chiffrement (Cryptographie) - Utiliser un algorithme reconnu et sûr, - Protéger les clés secrètes.

Tableau 16 : Les mesures de sécurité techniques

La liste proposée à travers le tableau précédent n'est pas exhaustive vu l'évolution permanente des mesures de sécurité à travers le temps. Nous avons cité les mesures essentielles qui peuvent garantir un minimum de sécurité dans une organisation. Ces mesures techniques sont

[19] Plan de reprise d'activité
[20] Plan de continuité d'activité

généralement mises en œuvre par le service informatique ou la DSI (Direction des Systèmes d'Information) de l'organisation. Les salariés au sein des organisations non pas forcément une connaissance suffisante de ces mesures techniques pour assurer une sécurité satisfaisante, c'est pour cela il existe des mesures organisationnelles et humaines complémentaires aux mesures techniques qui peuvent garantir un bon niveau de sécurité.

3. Les actions organisationnelles

Dans cette partie, nous allons présenter les mesures organisationnelles de sécurité, qu'une organisation peut les mettre en place afin d'assurer une sécurité satisfaisante de son SI. Des guides, méthodes ou normes pourront être utilisées, afin de mieux connaître les bonnes pratiques de la sécurité des informations ou du SI en général. Nous allons commencer tout d'abord avec la gestion des risques qui représente pour nous, une mesure très importante, voire primordiale.

3.1 La gestion des risques

Afin de bien gérer les risques liés à la sécurité des SI, il existe plusieurs méthodes d'analyse des risques en matière de sécurité des informations, parmi ces méthodes nous allons citer les plus connues et les plus utilisées en France :

Méthode	**Année**	**Source**	**Définition**
MARION	1984	Club d'utilisateurs (CLUSIF)	signifie Méthode d'analyse et de réduction des risques informatiques optimisés par niveau. Elle permet en quelques jours de réaliser une "photographie" de l'état de sécurité d'un système d'information à un instant donné. L'approche est réalisée grâce à des questionnaires et des données réactualisées annuellement, correspondant à l'activité sectorielle de l'entreprise. Elle a été adaptée à divers contextes informatiques, grands, moyens et petits systèmes. La méthode vise à réduire les vulnérabilités aux accidents, erreurs et malveillances afin d'assurer la sécurité en matière de disponibilité, d'intégrité et de confidentialité. (Lamère, 1985; Guinier, 1992).

MEHARI	1996	Club d'utilisateurs (CLUSIF)	Méthode Harmonisée d'Analyse du Risque Informatique, mais en réalité, nous nous trouvons plutôt face à un ensemble d'outils de management de la sécurité, une boîte à outils de laquelle on peut tirer, en fonction des besoins et des circonstances, la solution au problème posé en matière de management de la sécurité. (Barlette, 2005)
OCTAVE	1999	Universitaire (Carnegie Mellon)	Qui signifie en français, évaluation opérationnelle et critique des menaces, biens et vulnérabilités. Cette méthode prend en compte toutes les composantes du risque (biens informationnels, menaces, et vulnérabilités) contrairement à d'autres méthodes, qui ne disposent de ce fait pas d'informations suffisantes pour disposer d'une stratégie de protection adaptée.
ISO 27001	2005	ISO Certification de BS 7799-2	Cette norme définit les exigences pour la mise en place d'un système de management de la sécurité de l'information (SMSI) qui recense les mesures de sécurité, dans un périmètre défini, afin de garantir la protection des actifs de l'organisation. L'objectif est de protéger les informations de toute perte, vol ou altération, et les systèmes informatiques de toute intrusion et sinistre.

Tableau 17 : Méthode d'analyse et de gestion des risques en matière de sécurité des informations

Néanmoins, l'utilisation de ces méthodes présente des limites. Vu leurs lourdeurs, elles réclament une mobilisation importante de moyens humains et financiers et le processus reste très long. Ce qui peut décourager la plupart des PME à mettre en place de telles méthodes. Dans ce sens, Von Solms et Van de Haar (2000) pensent que la sensibilisation au sujet de la sécurité des informations est habituellement trop faible dans les PME pour déclencher l'adoption d'une méthode, et que les PME n'ont pas l'expertise suffisante pour conduire leur propre analyse de risque et n'ont pas les moyens de payer un consultant.

Les règlementations vont avoir un impact sur la gestion du risque ou même sur les pratiques de sécurité des S.I. en entreprise.

3.2 Les contraintes réglementaires

3.2.1 Les lois spécifiques au domaine informatique

Loi	Article	Contenu
Le code pénal	226-16	*« le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende*. »
RGPD (Règlement Général sur la protection des données)	N°2018-493	Relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Une mise en œuvre plus stricte et des amendes allant jusqu'à 4% du chiffre d'affaires total d'une entreprise, dans le but de décourager la violation des règles.
La loi pour la confiance dans l'économie numérique	N°2004-575	apporte un cadre juridique au commerce électronique et clarifie les relations entre les consommateurs et les fournisseurs. Elle définit notamment les éléments touchant à la sécurité des transactions en ligne et à la protection des droits individuels.

Tableau 18 : Lois spécifiques au domaine informatique

Ces lois obligent les entreprises à protéger leurs informations et principalement les informations nominatives. Certaines lois telles que la loi pour la confiance dans l'économie numérique pourraient aussi s'avérer être un frein à certains systèmes automatiques de sécurité.

3.2.2 Les lois provenant du secteur financier

Loi	Date d'application	Contenu
Loi Sarbanes-Oxley	2002	Imposant de nouvelles règles sur la comptabilité et la transparence financière. Elle fait suite aux différents scandales financiers. NB : La très grande majorité des PME françaises n'est pas concernée par cette loi.
Loi sur la sécurité financière	2003	La LSF concerne toutes les sociétés anonymes. Elle a mis en place le renforcement du contrôle interne afin de préciser les conflits d'intérêts et d'accroître la responsabilité des dirigeants.
La réglementation Bâle 3	2010	Est une réforme financière qui a pour but de renforcer la sécurité et la solidité du système bancaire.

Tableau 19 : Lois du secteur financier

L'application de ces trois règlementations permet un meilleur alignement entre la gestion des risques des entreprises et leur stratégie. Ces contraintes vont favoriser l'émergence de la gestion des risques informationnels des entreprises. Néanmoins, les PME sont très peu concernées par ces lois.

3.3 Le recours à l'assurance

Afin d'assurer leurs systèmes d'information, les entreprises peuvent faire recours aux assurances. Prenons l'exemple de l'assurance pour les voitures, pratiquement tout le monde possède une assurance pour sa voiture. Imaginons que cette assurance ne soit plus obligatoire, de nombreuses personnes arrêteraient de la payer en décidant de prendre le risque. En se disant que le nombre d'accidents est très faible et qu'un sinistre ne coûte pas si cher. Il suffit d'un accident entraînant la mort pour que cette équation parte en fumée. C'est le même principe en sécurité des SI, mais contrairement aux assurances automobiles, aucune loi n'oblige les entreprises à se protéger. Donc, les politiques de sécurité varient d'une entreprise à une autre. La sécurité est un compromis entre le risque et le coût que chaque entreprise évalue en fonction de ses priorités.

Les entreprises peuvent garantir à leur assureur qu'elles ont pris un minimum de précautions par l'intermédiaire d'un audit, ou encore le recours à une certification, ce qui reste problématique pour les PME. (Barlette, 2005).

3.4 La sécurité physique des équipements et locaux

Selon la Cnil, l'accès aux locaux doit être contrôlé pour éviter ou ralentir un accès direct, non autorisé, que ce soit aux fichiers papiers ou aux matériels informatiques, notamment aux serveurs. Parmi les mesures à mettre en place pour protéger les équipements et les locaux nous pouvons citer :

-Installation des alarmes anti-intrusion et les vérifier périodiquement.

-Mettre en place des détecteurs de fumée ainsi que des moyens de lutte contre les incendies.

-Protéger les clés qui permettent l'accès aux locaux et les codes d'alarme.

-Établir des règles et des moyens de contrôle d'accès des visiteurs, au minimum en faisant accompagner les visiteurs, en dehors des zones d'accueil du public.

-Distinguer les zones des bâtiments selon les risques, par exemple, prévoir un contrôle d'accès dédié pour les salles informatiques.

-Protéger physiquement les matériels informatiques par des moyens spécifiques comme les systèmes anti-incendie dédiés, surélévation contre d'éventuelles inondations, redondance d'alimentation électrique et/ou de climatisation, etc.

-Exigence du port d'un moyen d'identification visible (badge) pour toutes les personnes.

4. Les actions humaines : Sensibilisation, éducation et formation

Pour Keller et al. (2005), les employés en interne ont été identifiés comme présentant les plus importantes menaces pour la sécurité des informations. Et pour Pipkin, (2000), les salariés sont les principaux facteurs de détection d'une anomalie, avant même les systèmes informatisés de détection d'intrusion ou le service informatique. Donc, nous pouvons dire que les salariés constituent à la fois une faiblesse, qu'il faut limiter, et une force, qui doit être développée.

Kruger et Kearney, (2006) définissent la sensibilisation comme « *le degré ou l'étendue de la compréhension de la sécurité des informations par chaque membre du personnel, des niveaux de sécurité de l'information adéquats pour l'organisation, de leurs responsabilités individuelles face à la sécurité et de leurs comportements en adéquation*. »

Certains chercheurs ajoutent que si l'objectif derrière un programme de sensibilisation à la sécurité est d'améliorer l'importance de la sécurité des systèmes d'information, il permet aussi de limiter les effets négatifs possibles d'une faille dans la sécurité ou d'une panne (Hansche, 2001).

Quant à l'éducation et la formation à la sécurité, elles sont définies comme un processus d'apprentissage qui fournit des connaissances générales sur un certain sujet lié à l'environnement de sécurité et les compétences de sécurité requises pour que les employés exécutent les procédures de sécurité (Da Veiga et Martins, 2017).

Da Veiga (2015), propose une approche de formation et de sensibilisation à la sécurité de l'information (ISTAAP[21]) qui peut être utilisée pour inculquer une culture positive de la SSI qui aidera à s'attaquer au risque que le comportement humain représente pour la protection de l'information. Un outil d'évaluation de la CSSI est utilisé comme instrument de diagnostic critique pour évaluer la culture de la sécurité de l'information dans le contexte de l'ISTAAP.

Une étude de cas est discutée où l'ISTAAP (Figure 23) a été déployé. Cela a fourni des données empiriques pour illustrer la valeur de l'ISTAAP pour orienter le comportement des employés grâce à une formation et une sensibilisation ciblées basées sur les résultats des données d'évaluation de la culture de la sécurité de l'information.

La culture de la sécurité de l'information dans les cas étudiés est devenue plus positive au fil du temps, comme le montrent les données de l'ISCA[22] utilisé dans le cadre de l'ISTAAP. Une culture de sécurité de l'information plus positive se traduira par des employés qui adopteront des comportements averses au risque, introduiront moins d'incidents, se conformeront aux politiques et contribueront finalement à la protection des informations.

[21] Information Security Training And Awareness Approach
[22] Information Security culture Assessment

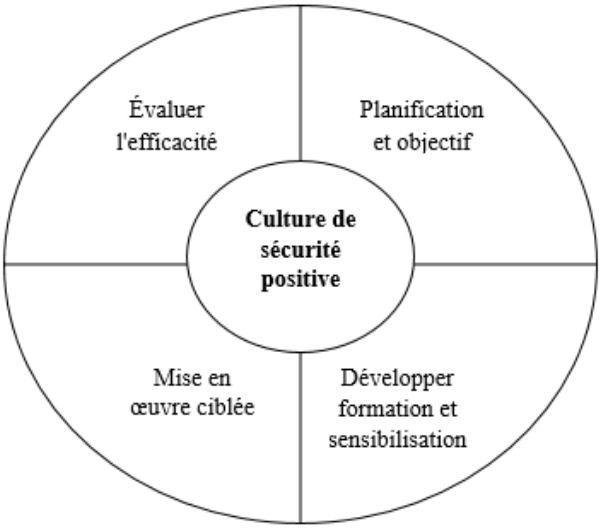


Figure 23 : Modèle de formation et de sensibilisation à la sécurité de l'information (ISTAAP) (adapté de Da Veiga, 2015)

Pour Da Veiga et Eloff, (2007), les organisations doivent veiller à ce qu'« *une culture de la sécurité de l'information soit inculquée par la formation, l'éducation et la sensibilisation, afin de minimiser les risques pour les actifs d'information*» . Cette implication est conforme à l'affirmation qu'une culture de sécurité efficace représente l'une des bases nécessaires à la gestion de la SSI et ne peut être atteinte sans une attention appropriée à la sensibilisation à la sécurité, à la formation et à l'éducation de tous les utilisateurs des TIC (Tarimo, 2006). Les entreprises peuvent être aidées à instaurer une culture de la sécurité grâce à diverses approches basées sur la politique, la sensibilisation, la formation et l'éducation (Furnell et al, 2001; Lichtenstein et Swatman, 2001; Lim et al, 2010; Schlienger et Teufel, 2003).

L'éducation des employés quant à leurs rôles et responsabilités en matière de sécurité est un aspect crucial de la culture de sécurité (R. von Solms et S. von Solms, 2004). La formation à la sécurité peut contribuer à la création d'une culture de sécurité en améliorant le comportement des employés et en augmentant leur niveau de sensibilisation à la sécurité. Cela pourrait se refléter dans leur comportement en matière de sécurité en suivant la politique de sécurité (Alnatheer et al, 2012).

Une étude de Chen et al (2015), propose un modèle qui évalue les influences des éléments-clés des programmes de sécurité de l'information (SETA[23]) sur la culture de la sécurité. Les résultats indiquent que la sensibilisation aux programmes SETA (Education, formation et

[23] (Security Education, Training, and Awareness) programs

sensibilisation) a une influence significative sur la culture de sécurité et sur les connaissances des employés.

Malgré l'importance de ces procédures dans l'amélioration de la culture de sécurité et des comportements liés à la sécurité des employés, une étude réalisée par Arthur Andersen, (2000), montre que peu d'entreprises mettent en place des campagnes de sensibilisation, et ces campagnes restent rares et insuffisantes. Et pour Keller et al. (2005) la sensibilisation et la formation apparaissent tout en bas de la liste des priorités des dépenses dans la sécurité des informations. Cela nous mène à nous interroger sur la situation ou la position des PME vis-à-vis de la sensibilisation et la formation. Est-ce qu'elles ont les moyens ? Est-ce qu'elles ont une conscience de l'importance de ces procédures ?

Pour Raymond, (1990) et Igbaria et al. (1997), les petites entreprises manquent de ressources pour mettre en place des centres d'information ou des formations et les campagnes de sensibilisation et de formation sont les premières à être annulées lors de coupures dans les budgets, du fait de la difficulté à faire apparaître leur bénéfice direct (Schultz, 2004).

Bien que les PME puissent avoir des difficultés pour mettre en place des programmes de sensibilisation et de formation à la sécurité de leurs SI, nous pensons que la première étape pour motiver les PME à mettre en place ces programmes c'est la sensibilisation de la direction des bénéfices qui peuvent résulter de ces programmes.

Une étude réalisée dans des PME par Kuusisto et Ilvonen (2003), montre que la formation permet de s'assurer que les gens prennent des mesures pour mettre à jour la documentation. L'apprentissage en ligne, la formation et l'éducation sont des initiatives potentiellement précieuses pour développer une culture de SSI pour les PME. Dojkovski et al (2007).

Synthèse de la section 3

Tout au long de cette section, nous avons montré comment une organisation peut être non sécurisée, à travers la présence des menaces, des vulnérabilités, des risques et la concrétisation des sinistres, en illustrant avec des exemples. Ensuite, pour faire face à ces différents dangers qui peuvent mettre en péril le SI d'une organisation, nous avons présenté les différentes mesures de sécurité qu'une organisation peut mettre en place, nous rappelons qu'un niveau de sécurité à 100% n'existe pas. Et surtout, nous montrons l'importance de la sensibilisation et la formation dans l'amélioration de la culture sécurité et les comportements liés à la sécurité des employés.

Conclusion du chapitre 1

La démarche théorique suivie dans ce chapitre en trois temps, a permis d'apporter un éclairage sur notre problématique générale.

Ce chapitre nous a permis de définir les contours de la culture sécurité (section 1), puis d'examiner les comportements liés à la sécurité et leur relation avec la culture sécurité (section 2) et les mesures à mettre en place afin de sécuriser une organisation (section 3).

Nous concluons, qu'une culture sécurité dans le domaine des SI dépend de plusieurs facteurs et déterminants qui peuvent varier d'une organisation à une autre selon la taille, le secteur d'activité, l'environnement général etc. Une culture de sécurité positive peut encourager les comportements liés à la sécurité tels que le changement régulier des mots de passe, la protection des données confidentielles, le respect de la politique de sécurité mise en place etc.

Pour affiner ces constats dans le but de construire notre propre modèle de recherche, il convient d'examiner les facteurs et les variables qui peuvent influencer ou former une culture de sécurité des SI au sein des PME. Le chapitre 2 va ainsi se focaliser sur ces facteurs et variables déterminants d'une culture sécurité des SI pour construire notre modèle de recherche qui va nous permettre de former nos orientations de recherche.

Chapitre 2
Construction d'un modèle conceptuel adapté à la PME et orientations de recherche

Le chapitre précédent fait état des approches théoriques qui offrent un cadre à l'étude des composants et des facteurs qui influencent la culture sécurité et les comportements liés à la sécurité des SI dans les organisations en général et dans les PME particulièrement. La revue de la littérature et les principales conclusions des travaux antérieurs sont prises en compte, dans ce chapitre, pour concevoir un modèle conceptuel original de recherche sur la culture sécurité de l'utilisateur du système d'information au sein de la PME. Pour répondre à cette finalité de modélisation de cette culture de sécurité, ce modèle consiste à garder, parmi de nombreux facteurs identifiés dans la littérature en culture sécurité, un ensemble de concepts appropriés au cadre organisationnel de la recherche. Il postule également un certain nombre de orientations qui supposent les relations entre ces concepts édifiant la problématique de la recherche. Dans ce sens, une démarche combinant une approche aussi bien théorique qu'empirique est sélectionnée. La construction théorique du modèle s'est réalisée à partir d'une revue de la littérature en ayant comme objectif la « justification » de la sélection de l'éventail des variables à partir des théories mobilisées dans le chapitre précédent. Ce chapitre s'articule autour de trois sections. La première section est dédiée à la précision des concepts du modèle conceptuel issue de la littérature. La deuxième section présente le modèle conceptuel proposé et les orientations de la recherche.

Section 1 : Précision des concepts du modèle

Section 2 : Modèle conceptuel et orientations de la recherche

Section 1 : Précision des concepts du modèle

L'objectif de cette section est de définir les concepts considérés dans le modèle de recherche. Il s'agit d'en préciser les soubassements et contributions pour évaluer le niveau de la culture sécurité de l'utilisateur du SI et comment améliorer en conséquence les comportements liés à la sécurité de cet utilisateur. Chaque concept fait ainsi l'objet d'une définition, en se référant aux fondements théoriques du chapitre précédent.

1. Définition des concepts du premier niveau conceptuel

La détermination et l'évaluation d'une culture sécurité des SI, exigent la considération d'un certain nombre de déterminants contextuels à même d'influencer les croyances des utilisateurs en ce qui concerne la sécurité du SI.

Le premier niveau du modèle conceptuel renvoie à l'évaluation des dimensions internes et externes à l'entreprise susceptibles d'influencer la culture sécurité d'un utilisateur du SI **(Niveau 2)** et en conséquence, de ses comportements liés à la sécurité **(Niveau 3)**. Dans ce sens, un certain nombre de facteurs sont mobilisés pour apprécier le contexte au sein duquel nous procédons à définir la culture sécurité des utilisateurs. . L'exploration et l'examen des effets de ces différents facteurs s'inscrivent dans une orientation managériale pragmatique de résolution des actions correctives nécessaires.

La prépondérance des facteurs qui influencent la culture sécurité a été mise en lumière par de nombreux travaux théoriques et empiriques appuyant des démarches d'évaluation de la culture sécurité (Dojkovski et al, 2006 ; Alnatheer et al, 2012 ; AlHogail et al, 2015 ; Tolah et al, 2017).

Trois catégories de facteurs qui influencent la culture sécurité de l'utilisateur d'un SI sont considérées dans cette recherche : les facteurs exogènes, les facteurs endogènes et enfin la direction. Une démarche considérant une approche à la fois théorique et empirique a permis de distinguer six facteurs, dont trois concernent les facteurs exogènes, deux touchent aux facteurs endogènes et enfin, un facteur lié concept de la direction. Ces facteurs sont décrits dans les sous-titres suivants.

1.1 Les facteurs exogènes

Ces facteurs exogènes impactent le niveau de la culture sécurité de l'utilisateur du SI. Ils représentent les stimuli externes à la PME, présumés influencer la culture sécurité. Cette catégorie de facteurs regroupe le contexte réglementaire et légal, le rôle de services (ou rôle des prestataires informatiques) et enfin, l'appartenance à un Secteur d'activité.

1.1.1 Le contexte réglementaire et légal

Le contexte règlementaire et légal joue un rôle important en matière de la sécurité des SI (Ismail et al, 2019), car des lois pourraient obliger les entreprises, à mettre en place les actions les plus indispensables. Comme par exemple, le nouveau règlement général sur la protection des données (RGPD) est un règlement de l'Union européenne qui constitue le texte de référence en matière de protection des données à caractère personnel, entré en vigueur le 25 mai 2018. Il renforce et unifie la protection des données pour les individus au sein de l'Union européenne. Et il oblige à terme les entreprises à mettre en place des procédures spécifiques, en accroissant le montant des amendes qui peuvent aller jusqu'à 1 million d'euros.

Une recherche récente de Mourrain et Leconte (2019) montre que l'obligation de la mise en application du RGPD génère une charge et un coût pour l'entreprise mais constitue une réelle opportunité pour les entreprises de types ETI[24] ou PME moins sensibles à la sécurité des SI que les grands groupes.

Un autre exemple, la charte de cybersécurité mise en place par la CCI[25] qui s'inscrit dans une démarche destinée à réduire les risques numériques tant au niveau des prestataires que de leurs clients.

Cette influence était présente dans des études sur la cybersécurité, telle que l'étude de Srinivas et al (2018) qui discute la stratégie nationale visant à sécuriser le cyberespace et de diverses politiques gouvernementales.

Pour Dojkovski et al (2007), les gouvernements peuvent jouer des rôles de soutien clés, à travers par exemple la distribution de brochures de sensibilisation à la SSI aux PME et la conduite de

[24] ETI : Entreprises de Taille Intermédiaire
[25] Chambre de Commerce et de l'Industrie

l'analyse comparative nationale de la SSI entre les PME, ou pour aider les organisations, des exemples de scénarios de risque de sécurité peuvent être développés à partir des ressources de sécurité existantes.

Pour l'utilisation des normes de SSI, parmi les PME de moins de 200 salariés, s'avère rare car elles sont généralement trop lourdes pour de petites structures (Barlette et Fomin, 2009). A défaut de normes, afin de les aider à adopter de bonnes pratiques, il faut informer les dirigeants de PME de l'existence de guides, comme celui de l'ANSSI[26] et la CPME[27] (2017), un guide[28] pour la SSI destiné aux PME.

Pour Barlette (2012), la voie juridique est prometteuse, car des lois pourraient obliger les dirigeants, même non impliqués, à mettre en place les actions les plus indispensables. Enfin, l'application d'un ensemble de normes et de réglementations de sécurité aurait un impact important sur le comportement de sécurité des utilisateurs (Alfawaz et al, 2010 ; Colella et al, 2014). De plus, les employés doivent être informés de la législation gouvernementale pertinente en matière de SSI (AlHogail et al, 2015).

1.1.1 Rôle des prestataires informatiques

Certaines PME choisissent d'externaliser plus ou moins globalement la gestion de leur système d'information. Comme par exemple le recourt à des petites structures ou à des indépendants. Et pour les plus grandes entreprises le recourt à des sociétés de services en ingénierie informatique (S.S.I.I). La PME peut avoir plusieurs intérêts d'une telle démarche, premièrement, elle peut bénéficier de compétences externes avec des expériences et connaissances plus étendues, ce qui lui permet d'éviter d'embaucher des informaticiens et de garder une souplesse au niveau de son effectif, deuxièmement, elle peut éviter de se disperser autour de son activité principale. Cette externalisation peut consister en un simple dépannage logiciel ou matériel, mais peut aussi s'étendre au conseil, voire même à la prise en charge complète de la gestion de son S.I. et de sa sécurité. (Barlette, 2005). Si le prestataire est amené à connaître des codes d'accès, s'il peut avoir accès à des données sensibles ou confidentielles il devient nécessaire pour la PME d'avoir une grande confiance dans son prestataire.

[26] ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information
[27] CPME : Confédération des Petites et Moyennes Entreprises
[28] https://www.ssi.gouv.fr/uploads/2017/01/guide_cpme_bonnes_pratiques.pdf

Mais le risque de cette externalisation est que la PME peut perdre la maîtrise de son S.I. ou de sa sécurité, il est donc nécessaire de pouvoir garder un contrôle en interne de ce qui est fait ou va être fait. (Barlette, 2005).

Le rôle du prestataire informatique n'a pas été suffisamment exploré dans les recherches en culture sécurité des SI. A notre connaissance, la seule étude qui a traité cet aspect, celle de Dojkovski et al, (2007), où ils affirment que les fournisseurs de technologies de SSI jouent des rôles-clés, dans le sens où ils peuvent fournir une sensibilisation à la SSI, mais ils peuvent également fournir une fiabilité aux PME qui, autrement, pourraient sentir qu'on leur vent du matériel et des logiciels inutiles.

1.1.2 Appartenance à un secteur d'activité

Il nous semble important de distinguer entre les PME techniques (appartenant aux secteurs de : l'informatique, télécommunications, services financiers…) des PME non techniques (appartenant aux autres secteurs d'activité), ces dernières peuvent avoir des problèmes plus graves en ce qui concerne la sécurité de leurs SI. D'autre part, il s'agit de distinguer les PME les plus sensibles à la confidentialité des données ainsi que celles qui dépendent fortement de la disponibilité et de l'intégrité de leurs informations (plateaux de télévente par exemple), ou bien des entreprises appartenant à des secteurs innovants ou de pointe (Barlette, 2012).
Une étude de Dagorn et Poussing (2012), en matière de gouvernance de la SSI, montre la difficulté à traduire les concepts en actions concrètes, appartenir au secteur de l'industrie comparativement au secteur des services.

Djokovski et al (2007), ont concentré leur étude sur des PME techniques qui employaient du personnel possédant des connaissances techniques. Alors que ces entreprises manquaient de cultures de SSI et étaient donc aptes à être étudiées, les PME non techniques peuvent avoir des problèmes plus graves, ce qui suggère la nécessité d'un soutien externe plus important. Pour ces chercheurs, ces entreprises non techniques pourraient être des sujets appropriés pour de futures études de cas interprétatives approfondies.

Donc, le secteur d'activité de la PME peut jouer un rôle important dans la prise de décision qui concerne la sécurité des SI et en conséquence sur le niveau de la culture sécurité de l'utilisateur des SI et sur les comportements liés à la sécurité de cet utilisateur.

1.2Les facteurs endogènes

Ces facteurs endogènes à l'entreprise impactent le niveau de la culture sécurité de l'utilisateur du SI. Ils représentent les stimuli internes à la PME, pouvant influencer la culture sécurité. Cette catégorie de facteurs regroupe la gestion des risques liés aux SI et les actions de formation et de sensibilisation à la sécurité des SI.

1.2.1 La gestion des risques

La gestion des risques liés aux SI à travers une analyse et une évaluation des risques, peut contribuer à une meilleure culture sécurité des SI au sein des PME.

De nombreux travaux (Eloff, 2002 ; Da Veiga et Eloff, 2010 ; Alnatheer, 2014 ; Tolah et al 2017) ont montré cette influence comme importante pour les grandes organisations.

Lorsque les contre-mesures sont adéquates pour réduire la probabilité de perte ; quand cela affecte un niveau acceptable et aide les organisations et ses employés à devenir capables de comprendre les dommages potentiels à la sécurité, ce qui contribue à créer une conscience de la culture de la SSI (Da Veiga et Eloff, 2010 ; Martins et Eloff, 2002).

Djokovski et al (2007) ont montré à travers une étude sur des PME Australiennes, que la gestion des risques par le biais des contremesures adéquates peut diminuer la probabilité de perte et aide la PME et ses employés à devenir capables de comprendre les potentiels dommages à la sécurité ce qui contribue à créer une prise de conscience envers la culture SSI. Une avenue potentiellement fructueuse suggérée par cette étude est de persuader les propriétaires de PME d'entreprendre un processus formel d'analyse des risques / protection des actifs informationnels basée sur des scénarios. Les résultats des enquêtes sur la SSI ont mis en évidence une forte corrélation entre le processus formel d'évaluation des risques et les dépenses consacrées à la SSI (ISBS 2006). Il est intéressant de noter que les experts ont également proposé un processus d'analyse holistique des risques basé sur l'entreprise afin d'élargir et de soulever la question de la SSI à un problème d'alignement stratégique de l'entreprise (Gerber & von Solms 2005). Les résultats d'une analyse des risques peuvent motiver une attitude proactive envers la gestion de la SSI (Djokovski et al, 2007), ce qui est en cohérence avec la théorie de la gouvernance des SI que nous avons déjà développée au niveau de notre premier chapitre.

Dans les lignes directrices de l'OCDE (2002), régissant la sécurité des systèmes et réseaux d'information (vers une culture de la sécurité), parmi les neuf principes exposés nous trouvons l'évaluation des risques qui « *permet de déceler les menaces et vulnérabilités et doit être suffisamment large pour couvrir l'ensemble des principaux facteurs internes et externes, tels la technologie, les facteurs physiques et humains, les politiques et services de tierces parties ayant des implications sur la sécurité. L'évaluation des risques permettra de déterminer le niveau acceptable de risque et facilitera la sélection de mesures de contrôle appropriées pour gérer le risque de préjudices possibles pour les systèmes et réseaux d'information compte tenu de la nature et de l'importance de l'information à protéger* ». (OCDE, 2002).

Pour conclure, nous considérons que la gestion des risques liés aux SI au sein de la PME, peut avoir une influence sur le niveau de la sécurité des SI et en conséquence sur le niveau de la culture sécurité de l'utilisateur et de ses comportements liés à la sécurité.

1.2.2 Actions de formation/sensibilisation

Une formation à la sécurité pour les employés aura une influence positive sur leur culture sécurité. (Dojkovski et al, 2007 ; Alnatheer, 2012 ; Da Veiga, 2015).

La formation et l'éducation sont des initiatives potentiellement intéressantes pour développer une culture de SSI pour les PME, comme cela a également été constaté pour les grandes entreprises par (Furnell & Clarke 2005 ; Furnell et al. 2004 ; Siponen 2000).

Le partage des connaissances, la coopération et la collaboration ont été jugés importants pour l'apprentissage aux niveaux individuel et organisationnel afin de développer une culture de SSI en PME. (Djokovski et al, 2007).

La formation à la sécurité peut contribuer à la création d'une culture de sécurité en améliorant le comportement des employés et en augmentant leur niveau de sensibilisation à la sécurité. Cela pourrait se refléter dans leur comportement en matière de sécurité en suivant la politique de sécurité (Alnatheer et al, 2012).

Une sensibilisation à la sécurité forme un pilier pour la mise en place d'une culture sécurité. (Hassan et Ismail, 2012 ; Da Veiga et Martins, 2015 ; Tolah et Al, 2017).

Kruger et Kearney, (2006) définissent la sensibilisation comme « *le degré ou l'étendue de la compréhension de la sécurité des informations par chaque membre du personnel, des niveaux*

de sécurité de l'information adéquats pour l'organisation, de leurs responsabilités individuelles face à la sécurité et de leurs comportements en adéquation. »

Certains chercheurs ajoutent que si l'objectif derrière un programme de sensibilisation à la sécurité est d'améliorer l'importance de la sécurité des systèmes d'information, il permet aussi de limiter les effets négatifs possibles d'une faille dans la sécurité ou d'une panne (Hansche, 2001).

Une étude de Barlette (2005), sur les comportements liés à la sécurité dans les PME suggère qu'une sensibilisation (information et éducation) et/ou une formation pourraient être lancées afin de limiter les failles identifiées (faiblesse des mots de passe, manque de sauvegarde, fuite des données etc.). Une telle intervention pourrait s'avérer courte et donc peu coûteuse car ce sont surtout des principes basiques qu'il faudrait transmettre aux salariés.

Da Veiga et Eloff, (2007), affirment que les organisations doivent veiller à ce qu'« *une culture de la sécurité de l'information soit inculquée par la formation, l'éducation et la sensibilisation, afin de minimiser les risques pour les actifs d'information* ».

Une étude récente de Chen et al (2015), où ils proposent un modèle qui évalue les influences des éléments-clés des programmes de SSI sur la culture de la sécurité. Les résultats indiquent que la sensibilisation aux programmes (Education, formation et sensibilisation) a une influence significative sur la culture de sécurité et sur les connaissances des employés.

Donc, nous considérons la formation et la sensibilisation comme des éléments internes à la PME qui peuvent amélioré considérablement le niveau de la culture sécurité de l'utilisateur du SI et de ses comportements liés à la sécurité.

1.3 La direction

Nous désignons par direction, la sensibilité du dirigeant à la sécurité des SI de son entreprise qui se réfère selon, Martin et Da Veiga, (2015) à un degré de la compréhension par la haute direction de l'importance de la fonction de SSI et participe aux activités de sécurité visant à améliorer et à créer une forte culture de la sécurité de l'information. Et le degré d'engagement de la direction en ce qui concerne la sécurité (Budget alloué, intérêt à la sécurité, mesures de sécurité prises etc.). Nous avons consacré à la direction, une catégorie distincte de la catégorie des facteurs endogènes, malgré que la direction fait partie de ces facteurs endogènes, nous avons fait ce choix, parce que la direction joue un rôle clé dans le domaine de la sécurité des SI. Pour

Archimbaud et Longeon, (1999), « *la détermination et la supervision de la politique de sécurité sont des fonctions de direction. Rien de valable ne peut se faire sans le directeur* ». Et selon, Robinson et Volonino, (2004), le dirigeant serait le point de départ, en confirmant ceci : « *obtenir l'attention et l'implication du management afin de prendre en charge la gestion des risques organisationnels est la première étape de la prise en compte de la sécurité* ».
Surtout dans le cas des PME, où le top management se résume au dirigeant, car la majorité des petites entreprises ont une structure organisationnelle plate et sont gérées par le propriétaire qui est souvent le directeur (Solomon, 1986). Donc, les PME sont caractérisées par de petites unités de gestion plus autonomes, peu matures et dépendantes de l'expertise et des expériences du dirigeant (Winston et Heiko, 1990).

Pour Schein, (1990), le rôle du dirigeant est très important dans la mise en œuvre d'une culture et le changement de la culture. De plus, pour Fourcade et Marchesnay (1997), le dirigeant se conduit souvent en « père de famille » et a tendance à faire partager ses valeurs personnelles aux membres de son entreprise. Et selon (Hu et al. 2012), les actions du dirigeant dans la sécurité des SI sont essentielles pour réduire les risques et garantir la conformité des employés à la SSI. Donc, l'implication et la propension à agir des salariés sont directement dépendantes de celles du décideur (Forcht et Ayers, 2000 ; Barlette, 2005).

Fourie (2003) a indiqué que la haute direction peut être impliquée en définissant et en communiquant une politique de sécurité, en attribuant des responsabilités spécifiques aux personnes désignées, en mettant à disposition des ressources pour l'entretien continu de la sécurité et du contrôle de l'information, et en surveillant et en examinant constamment l'efficacité de la SSI. De nombreux chercheurs ont montré que la haute direction est un élément essentiel de l'établissement d'une culture de sécurité (Tessem et Skaraas, 2005 ; Kraemer et Carayon, 2007 ; Dojkovski et al, 2007 ; Alnatheer et al, 2012, 2014 ; Sherif et al, 2015 ; Martin et Da Veiga, 2015 ; Tolah et al, 2017).

Gaunt (2000) a soutenu que lors de la création d'une culture de la SSI, l'engagement de la direction et un leadership fort sont nécessaires à un stade initial pour réussir à long terme. En outre, Knapp et al (2006) ont constaté que le support de la direction est le prédicteur le plus important de la culture de sécurité et du niveau d'application des politiques de sécurité. Une culture de la sécurité ne serait pas facilement établie sans une implication forte et cohérente de la haute direction de l'organisation.

Tous ces arguments, montrent le rôle clé qui peut être joué par la direction de la PME afin de garantir un niveau acceptable de sécurité de leur SI ainsi qu'une culture sécurité positive des utilisateurs SI. La sensibilité du dirigeant à la sécurité peut se manifester par de nombreux indicateurs. Ceux retenus dans le cadre de cette recherche sont : le budget consacré à la sécurité, intérêt à la sécurité, mesures de sécurité déjà prises au sein de la PME, et le rôle exercé par le dirigeant pour impliquer les utilisateurs.

2. Définition des concepts du deuxième niveau conceptuel

Lors de notre revue de littérature sur la culture sécurité des SI, nous avons identifié des travaux (Alnatheer et al, 2012 ; Tolah et al, 2017) qui ont classé les facteurs de la CSI en deux types, des facteurs qui constituent la CSI et des facteurs qui l'influencent. Dans ce deuxième niveau de notre modèle, nous présentons les facteurs qui constituent la culture sécurité des SI, ou autrement dit, les niveaux qui composent la culture sécurité des SI.

Donc, ce niveau fait état des composants d'une culture sécurité des utilisateurs des SI. Grâce à ces composants, nous pouvons déterminer le niveau de la culture sécurité. Trois composants sont identifiés : la conscience de sécurité, la propriété de sécurité et la conformité à la sécurité. Nous allons détailler ces trois composants dans les titres ci-dessous.

2.1 Propriété de sécurité (Security ownership)

La propriété de sécurité ou en anglais « Security ownership » : fait référence à la façon dont les employés perçoivent leurs responsabilités, leurs rôles et leur volonté d'agir de manière constructive pour améliorer leurs propres performances en matière de sécurité et celles de l'organisation (Alnatheer et al, 2012). Dans les lignes directrices de l'OCDE (2002), « *les parties prenantes sont tributaires de systèmes et réseaux d'information locaux et mondiaux interconnectés. Elles doivent comprendre leur responsabilité dans la sécurité de ces systèmes et réseaux et en être, en fonction du rôle qui est le leur, individuellement comptables. Ces parties prenantes doivent régulièrement examiner et évaluer leurs propres politiques, pratiques, mesures et procédures pour s'assurer qu'elles sont adaptées à leur environnement. Celles qui développent, conçoivent et fournissent des produits et services doivent prendre en compte la sécurité des systèmes et réseaux et diffuser des informations appropriées, notamment*

des mises à jour en temps opportun de manière à ce que les utilisateurs puissent mieux comprendre les fonctions de sécurité des produits et services et leurs responsabilités en la matière ». (OCDE, 2002).

Il est important que le personnel de toute organisation comprenne leurs rôles et responsabilités en matière de sécurité, afin d'améliorer leurs performances et donc les performances de sécurité de l'organisation. En comprenant leurs responsabilités et l'importance de protéger la sécurité des SI, le personnel est en mesure de comprendre les risques de sécurité associés à leurs actions. Cela augmentera leurs niveaux de conscience de sécurité, ce qui augmentera la conformité avec les mesures de sécurité mises en œuvre dans l'organisation. Pour cette raison, la responsabilité des employés et l'appropriation du besoin de protéger les SI est un aspect important de la création d'une culture de la sécurité (Koh et al. 2005 ; Maynard et Ruighaver, 2002 ; Ramachandran et al. 2004 ; Tarimo, 2006). En étant responsable et en ayant un sentiment d'appartenance, le comportement du personnel changera en ce qui concerne la protection des actifs de l'organisation, conduisant à la création d'une culture de sécurité.

Nous signifions par propriété de sécurité, quand l'utilisateur exprime un intérêt à la sécurité des SI en premier lieu, ensuite s'il admet qu'il a une part de responsabilité dans la sécurité des SI de son entreprise, en commençant par son poste de travail et les données qui concernent son périmètre de responsabilité et en passant par le sens de responsabilité envers la sécurité de son entreprise.

2.2 Conscience de sécurité (Security awareness)

La conscience de sécurité ou « security awareness » en anglais, défini lorsque les utilisateurs comprennent les problèmes potentiels liés à la SSI et prennent conscience de l'importance de leur rôle en matière de sécurité. C'est ce qui mène à leurs engagements sur ce sujet (Da Veiga et Martins, 2017).

Siponen (2000) a défini la conscience de sécurité comme « *un état dans lequel les utilisateurs d'une organisation sont conscients, idéalement engagés, de leur mission de sécurité* ». La conscience de sécurité a été bien reconnue dans la littérature comme étant une composante essentielle de la création d'une culture de sécurité.

Von Solms (2000) évoque la troisième vague de SSI, appelée vague d'institutionnalisation, souvent évoquée sous le titre «Conscience de sécurité» et plus récemment sous le titre «culture de la SSI». Les chercheurs ont qualifié la culture de sécurité d'étape avancée de la conscience de sécurité (Alnatheer et al, 2012).

L'instauration d'une culture de sécurité passe par la conscience, les connaissances et les compétences en matière de sécurité (Tarimo, 2006). L'importance de la conscience de sécurité pour l'établissement d'une culture de sécurité a été reconnue par d'autres chercheurs dans la littérature, par exemple, van Niekerk et von Solms (2005) affirment que la culture de sécurité étant étroitement liée au comportement de sécurité, l'analyse des niveaux de conscience de la sécurité contribuera directement à l'établissement et au maintien d'une culture de sécurité. La norme ISO / CEI stipule que la conscience de sécurité de tous les employés est un élément essentiel d'une sécurité efficace et contribue positivement à une culture de sécurité améliorée (Organisation internationale de normalisation ISO / CEI TR 13335-1, 2004).

Dans cette recherche, nous désignons par conscience de sécurité tout ce qui est la connaissance des mesures de sécurité prises au sein de la PME, ça veut dire, est-ce que l'utilisateur connaît les mesures de sécurité mis en œuvre dans l'entreprise ? Ensuite, la connaissance des menaces, ça veut dire si l'utilisateur a conscience des menaces possibles qui peuvent mettre le système d'information de l'entreprise en danger, et aussi, si l'utilisateur a conscience comment se protéger ou comment faire face aux menaces de sécurité.

2.3 Conformité à la sécurité (Security compliance)

La connaissance par le personnel de la politique et des procédures de sécurité aura un impact positif sur leur attitude vis-à-vis des politiques de sécurité et sur la conformité. Dans une organisation où il existe une culture de sécurité forte ou saine, on s'attendrait à ce que la conformité soit un trait visible de la culture. (Veiga et Martins, 2017).

Selon Cheng et al. (2013), la politique de SSI est une déclaration écrite qui définit les exigences de la gestion de la sécurité organisationnelle. C'est la responsabilité et les obligations des employés, les sanctions et les contre-mesures en cas de non-respect. Plus encore, Vance et al. (2012) ont discuté du fait que la gravité perçue affecte positivement l'intention des employés

de se conformer aux politiques de sécurité, et les praticiens doivent s'assurer que les employés reconnaissent les menaces et les risques liés à la sécurité.

Néanmoins, la transformation des comportements de sécurité va au-delà de l'acquisition de connaissances sur les politiques de sécurité et de la prise de conscience de l'importance de la sécurité. Les recherches sur la conformité aux politiques de sécurité (par exemple, Bulgurcu et al. 2010 ; D'Arcy et al. 2009 ; Herath et Rao, 2009b) indiquent que, pour influencer le comportement de sécurité des utilisateurs, il faut affecter la manière dont les utilisateurs perçoivent les risques et prennent des décisions liées à la sécurité. Les programmes de sensibilisation doivent aller au-delà de la simple communication d'informations liées à la sécurité et s'aligner sur le processus de prise de décision individuelle.

Le rôle de la conscience de sécurité en tant qu'antécédent de la conformité a été identifié par Haeussinger et Kranz (2013), qui ont constaté que la conscience de sécurité influence les intentions des utilisateurs de se conformer aux politiques de sécurité, et pour €Arcy et coll. (2009) la conscience de sécurité est associée à la perception de l'utilisateur des sanctions (par certitude perçue et sévérité perçue des sanctions), qui à son tour détermine la conformité de l'utilisateur.

Alnatheer (2012), qui a parlé de deux facteurs qui composent la culture sécurité et ensuite il a proposé un autre élément important qui conceptualise la culture de sécurité qui est la conformité à la sécurité qui doit être prise en compte selon cet auteur pour créer une culture de sécurité.

Nous remarquons ici une confusion potentielle entre le comportement de sécurité et la conformité à la sécurité. Donc, quelle différence entre ces deux concepts ?

La conformité à la sécurité c'est des faits visibles mais non encore interprétés, ça veut dire que cette conformité va se traduire par des comportements de sécurité, par exemple, un salarié qui participe à une formation liée à la sécurité, ou s'il a lu une charte de sécurité ou une politique de sécurité ici il s'est conformé à la sécurité, cette conformité va peut-être se transformer en comportement de sécurité telle que l'application des mesures de sécurité recommandés lors de la formation ou inscrites sur la charte, par exemple le changement régulier des mots de passe, les sauvegardes, la protection des données confidentielles etc. Mais si un salarié s'est conformé à la sécurité, qu'il a assisté à une formation ou il a lu une charte de sécurité puis ensuite, n'a manifesté aucun comportement de sécurité, dans ce cas, nous parlons d'une conformité et non plus d'un comportement de sécurité effectif.

Nous avons tiré l'explication de cette différence entre ces deux concepts à partir du modèle des trois niveaux de culture de (Shein, 1985), que nous allons détailler son apport à notre cadre théorique dans le sous-titre suivant.

2.4 Intégration des approches théoriques : l'apport du modèle des trois niveaux de culture (Schein, 1985)

Selon Schein (1985), une culture peut être analysée à plusieurs niveaux différents, le terme niveau signifiant le degré auquel le phénomène culturel est visible pour l'observateur. Une partie de la confusion entourant la définition de ce qu'est réellement la culture résulte de la non-différenciation des niveaux auxquels elle se manifeste.

Ces niveaux vont des manifestations très tangibles que nous pouvons voir et ressentir à la base profondément ancrée, inconscientes hypothèses que Schein définit comme l'essence de la culture. Entre ces couches sont diverses croyances, valeurs, normes et règles que les membres utilisent comme moyen de représenter la culture pour eux-mêmes et pour les autres.

Les principaux niveaux d'analyse culturelle comme conçus par Schein sont présentés dans la figure suivante :

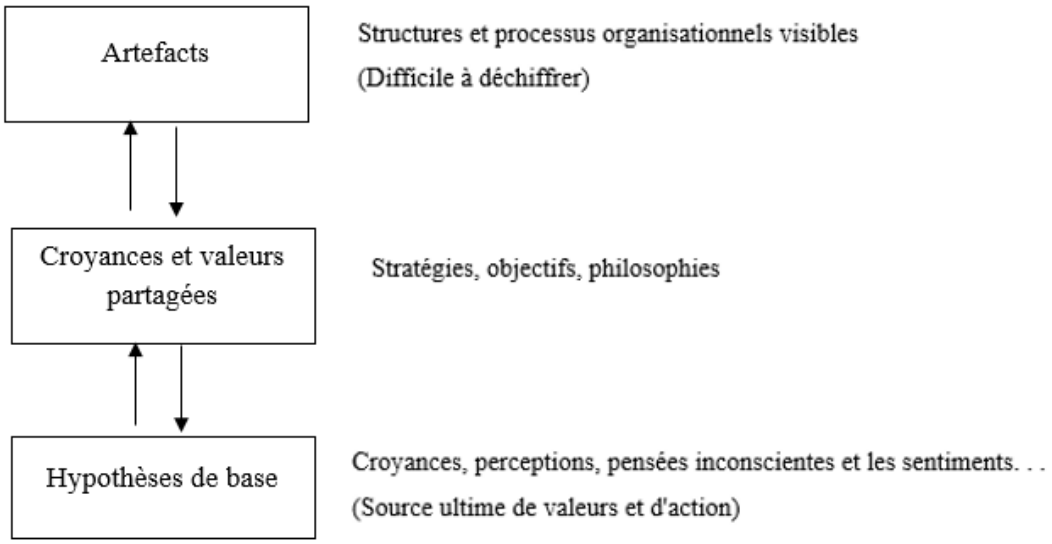


Figure 24 : Niveaux de culture (Schein, 1985)

2.4.1 Précisions relatives aux différents niveaux de culture

2.4.1.1 Les artefacts

À la surface se trouve le niveau des artefacts, qui comprend tous les phénomènes que l'on voit, entend et ressent quand on rencontre un nouveau groupe avec une culture inconnue. Les artefacts incluent le visible les produits du groupe, tels que l'architecture de son environnement physique ; sa langue, sa technologie et ses produits, les créations, son style incarné dans les vêtements, les manières d'adresse, démonstrations émotionnelles, mythes et histoires racontés sur l'organisation etc. (Schein, 1985).

Les artefacts incluent aussi les processus organisationnels par lesquels un tel comportement est rendu routinier, et des éléments structurels tels que des chartes, des descriptions formelles du fonctionnement de l'organisation et des organigrammes. Si l'observateur vit assez longtemps dans le groupe, la signification des artefacts devient de plus en plus claire. Si, cependant, on veut atteindre ce niveau de compréhension plus rapidement, on peut tenter d'analyser les valeurs, les normes et les règles adoptées qui fournissent les principes de fonctionnement selon lesquels les membres du groupe guident leur comportement. (Schein, 1985). Ce qui nous mène au prochain niveau d'analyse de la culture.

2.4.1.2 Les croyances et valeurs partagées

Tout apprentissage en groupe reflète en fin de compte les croyances et les valeurs de quelqu'un, leur sens de ce qui devrait être, par opposition à ce qui est. Lorsqu'un groupe est créé pour la première fois ou lorsqu'il est confronté à une nouvelle tâche ou un problème, la première solution proposée pour y faire face reflète les propres hypothèses de certains individus sur ce qui est bien ou mal. (Schein, 1985).

Les croyances et les valeurs ne sont pas fondées sur un apprentissage antérieur, elles peuvent aussi refléter uniquement ce qu'Argyris et Schön (1978) ont appelé «Espoused theories », qui prédisent ce que les gens diront dans une variété de situations mais qui peuvent ne pas correspondre à ce qu'elles seront dans les situations où ces croyances et valeurs devraient

fonctionner. Par exemple, une entreprise peut dire qu'elle valorise les gens et qu'elle a des normes de qualité élevées pour ses produits, mais son bilan peut contredire ce qu'elle dit. Un autre exemple, un utilisateur peut prédire qu'il a des connaissances en sécurité des SI et qu'il peut réagir en cas de problème de sécurité, alors qu'en vérité et en cas de problème, cet utilisateur peut ne pas agir convenablement pour faire face au problème de sécurité survenu.

Si les croyances et les valeurs adoptées sont raisonnablement en accord avec les hypothèses de base, l'articulation de ces valeurs dans une philosophie de fonctionnement peut être utile pour amener le groupe à agir ensemble. (Schein, 1985).

Pour atteindre ce niveau de compréhension plus profond, pour déchiffrer la culture, et pour prédire correctement le comportement futur, il faut comprendre plus complètement le niveau suivant, qui est les hypothèses de base.

2.4.1.3 Les hypothèses de base

À ce niveau, lorsqu'une solution à un problème fonctionne à plusieurs reprises, elle est prise pour acquis. Ce qui était autrefois une hypothèse, soutenue uniquement par une intuition ou une valeur, vient progressivement à être traité comme une réalité. Nous en venons à croire que la nature fonctionne vraiment de cette façon. (Schein, 1985).

Pour cet auteur, la culture comme un ensemble d'hypothèses de base définit pour nous à quoi prêter attention, ce que les choses signifient, comment réagir émotionnellement à ce qui se passe, et quelles mesures prendre dans divers types de situations.

Le pouvoir de la culture découle du fait que les hypothèses sont partagées et, par conséquent, mutuellement renforcées. Dans ces cas, probablement seulement un tiers ou une éducation interculturelle pourrait aider à trouver un terrain d'entente sur lequel les parties pourraient apporter leurs hypothèses implicites à la surface.

Pour Schein, la culture de n'importe quel groupe peut être étudiée à ces trois niveaux : niveau de ses artefacts, le niveau de ses croyances et valeurs adoptées, et le niveau de ses hypothèses de base. Si on ne déchiffre pas le modèle d'hypothèses de base, on ne saura pas comment interpréter correctement les artefacts ou quelle crédibilité donner aux valeurs articulées. Autrement dit, l'essence d'une culture réside dans les hypothèses de base, et une fois qu'on les

comprend, on peut facilement comprendre les autres niveaux plus superficiels et les traiter de manière appropriée.

Si nous revenons à la théorie des trois niveaux de la culture sécurité de Schein (1985), nous constatons que chaque facteur qui constitue la culture sécurité (Niveau 2 du modèle conceptuel) correspond à un niveau de culture proposé par Schein. D'où la propriété de sécurité correspond aux hypothèses de bases, la conscience de sécurité correspond aux valeurs partagées et enfin la conformité à la sécurité qui correspond aux artefacts comme présentés au niveau de la figure 25 et expliqué ci-dessous :

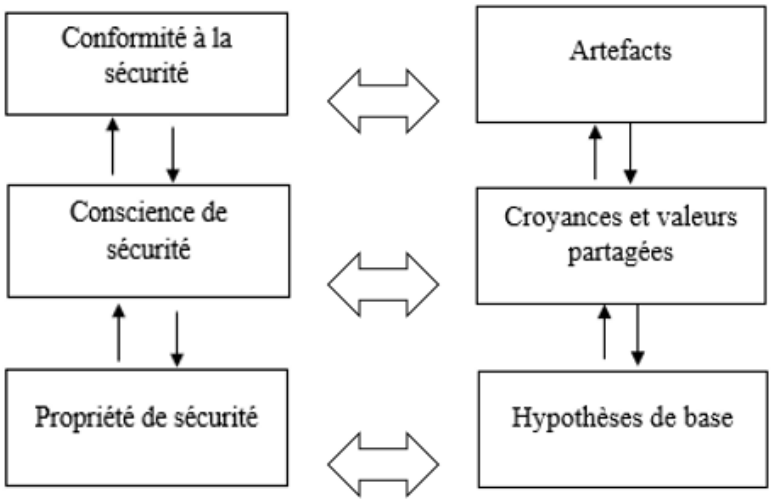


Figure 25 : Positionnement des facteurs qui constituent la culture sécurité des SI sur les trois niveaux de culture

Hypothèses de bases et propriété de sécurité

Pour Schein (1985), la culture comme un ensemble d'hypothèses de base définit pour nous à quoi prêter attention, ce que les choses signifient, comment réagir émotionnellement à ce qui se passe, et quelles mesures prendre dans divers types de situations. Nous estimons que la propriété de sécurité peut être placée sur le premier niveau de culture ''Hypothèses de base'', cette propriété de sécurité fait référence à la façon dont les employés perçoivent leurs responsabilités, leurs rôles et leur volonté d'agir de manière constructive pour améliorer leurs propres performances en matière de sécurité et celles de l'organisation (Alnatheer et al, 2012).

Valeurs partagées et conscience de sécurité

La conscience de sécurité, définit lorsque les utilisateurs comprennent les problèmes potentiels liés à la SSI et prennent conscience de l'importance de leur rôle en matière de sécurité. C'est ce qui mène à leurs engagements sur ce sujet (Da Veiga et Martins, 2017). Nous avons situé cette conscience dans le deuxième niveau de culture de valeurs partagées qui représentent tout apprentissage en groupe qui reflète les croyances et les valeurs de quelqu'un, leur sens de ce qui devrait être. Schein (1985).

Artefacts et conformité à la sécurité

À la surface se trouve le niveau des artefacts, qui comprend tous les phénomènes que l'on voit, entend et ressent quand on rencontre un nouveau groupe avec une culture inconnue. Les artefacts incluent aussi les processus organisationnels par lesquels un comportement est rendu routinier, et des éléments structurels tels que des chartes, des descriptions formelles du fonctionnement de l'organisation et des organigrammes. Si l'observateur vit assez longtemps dans le groupe, la signification des artefacts devient de plus en plus claire Schein (1985).
Dans ce niveau de culture nous avons situé la conformité à la sécurité, Selon, Da Veiga et Martins, (2017), dans une organisation où il existe une culture de sécurité forte ou saine, on s'attendrait à ce que la conformité soit un trait visible de la culture. La conformité se traduit par la connaissance par le personnel de la politique et des procédures de sécurité.

3. Le troisième niveau du modèle conceptuel

Dans ce troisième niveau de notre modèle de recherche, nous discutons les comportements liés à la sécurité de l'utilisateur des SI (Niveau 3) qui en résulte de la culture sécurité (Niveau 2) influencé elle-même par des facteurs externes et internes (Niveau 1).

Parmi les travaux qui ont cherché à comprendre les comportements liés à la sécurité des acteurs dans les PME nous citons ceux d'Yves Barlette (2006) où il distingue les comportements des dirigeants, et les comportements des salariés à travers une étude réalisée au sein de huit PME Françaises. Pour cet auteur, les principaux résultats sur les comportements des utilisateurs se résument comme suit : Les caractéristiques personnelles sont le principal moteur des comportements liés à la sécurité dans les PME. Les six facteurs les plus importants étaient les

motivations personnelles, la préservation de l'intimité, les motivations liées au poste, les motivations liées à l'entreprise, l'habitude et le vécu. Et les limitations des comportements liés à la sécurité des salariés sont principalement liées au manque de temps, autrement dit, à l'équilibre entre le temps de travail et le temps qui peut être affecté aux comportements liés à la sécurité. Les limitations sont aussi liées à un manque d'information, de sensibilisation et de formation, ce qui peut être dû à des problèmes de temps disponible, et plus globalement un problème de ressources financières au sein de la PME.

Selon l'Agence nationale de la sécurité des systèmes d'information (ANSSI) il faut avant tout adopter un bon comportement de sécurité en entreprise, parmi les comportements cités par cette agence dans son guide destiné aux PME nous trouvons : L'utilisation des mots de passe de qualité difficiles à retrouver et difficiles à deviner, effectuer des sauvegardes régulières, contrôler la diffusion d'informations personnelles et des données de l'entreprise etc.

Selon Pérès et Latour (2000), la notion de comportement lié à la sécurité d'un utilisateur de systèmes d'information regroupe cinq actions qui relèvent de la seule volonté des personnes : choisir un mot de passe difficile à découvrir par une autre personne ; interrompre la communication en quittant son poste de travail ; ne pas divulguer ou afficher son code d'accès ainsi que son mot de passe ; ranger des documents confidentiels dans un endroit sûr.

Parsons et al (2014), proposent un outil qui mesure les comportements de sécurité dans sept domaines d'intervention, à savoir, la gestion des mots de passe, l'utilisation d'e-mail, l'utilisation d'Internet, l'utilisation des réseaux sociaux, les appareils mobiles, le traitement de l'information et le rapport d'incident. Nous allons citer quelques exemples d'items parmi 21 items proposés par ces chercheurs et qui mesurent le comportement de sécurité :

- J'utilise un mot de passe différent pour mes réseaux sociaux et mes comptes professionnels,

- Je n'ouvre pas de pièce jointe si l'expéditeur m'est inconnu,

- Lorsque je travaille dans un lieu public, je laisse mon ordinateur portable sans surveillance.

Donc, à ce niveau du modèle, nous nous intéressons au comportement effectif, que nous le distinguons de l'intention de comportement qui est une mesure de la force de l'intention d'exercer un comportement spécifique, qui dépend des attitudes et des normes subjectives, tels que distingués dans la TRA (Theory of Reasoned Action, ou la théorie de l'action raisonnée) de (Davis et al. 1989) et dans la TBP (Theory of Planned Behavior, ou la théorie de prévision du comportement) de (Ajzen, 1991).

Dans le champ des SI, les comportements effectifs liés à la sécurité peuvent être par exemple : choisir un mot de passe robuste, la sauvegarde régulière des informations, le lancement régulier des mises à jour et des antivirus, ou encore fermer son bureau à clé.

Barlette (2006), distingue les comportements liés à la sécurité dits « positifs » des comportements dits « négatifs ». Pour lui un comportement « positif » des acteurs sera un comportement en conformité avec les règles de sécurité existantes dans l'entreprise, qu'elles soient écrites, contractuelles ou non, ou qu'elles soient verbales. Ce comportement inclura les initiatives personnelles supplémentaires prises, par exemple, les sauvegardes redondantes, le changement de mot de passe non demandé etc. A l'inverse, un comportement sécuritaire « négatif » sera lié à un non-respect de ces règles, que ce soit un comportement lié à une perte de temps, par exemple, utilisation de l'Internet à des fins personnelles, ou un contournement des mesures de sécurité existantes.

Pour résumer, nous étudions dans ce niveau de notre modèle, les comportements liés à la sécurité du SI, notre objectif est de comprendre si les comportements des utilisateurs sont propices à minimiser les risques et conforment aux mesures de sécurité ou à l'opposé, peuvent augmenter les risques pesant sur le SI de l'entreprise.

Le modèle conceptuel proposé fait état de relations qui consistent à décrire les déterminants et les composants de la culture sécurité. Les concepts mobilisés dans ce modèle sont donc exploités pour corroborer les différentes orientations de la recherche et produire des éléments de réponse à notre question de recherche « *Comment insuffler une culture sécurité des systèmes d'information en PME ?* ». Il importe alors, dans le titre suivant, de compléter la présentation du cadre conceptuel par la formulation des orientations de la recherche.
Les concepts mobilisés pour le contexte de cette démarche d'étude de la culture sécurité des SI sont récapitulés dans le tableau suivant :

Niveau conceptuel	Catégorie	Concept	Définition	Référence, Théorie ou modèle associé
Facteurs qui influencent la culture sécurité	**Facteurs exogènes**	Contexte réglementaire et légal	Regroupe tout ce qui est lois et règlements sur la sécurité des SI ou sur la protection des données comme par exemple l'RGPD, les chartes et les guides de cybersécurité et sécurité des SI.	Mourrain et Leconte (2019) ; Srinivas et al (2018) ; Colella et al (20014) ; Barlette (2012) ; Alfawaz et al (2010) ; Dojkovski (2007).
		Rôle des prestataires informatiques	C'est le rôle exercé par les prestataires informatiques, l'infogérance, les sociétés de services en ingénierie informatique (S.S.I.I) etc. dans la gestion de la sécurité des SI de la PME.	- Cadre conceptuel holistique de Dojkovski (2007) ; Barlette (2005).
		Appartenance à un Secteur d'activité	C'est la distinction entre les PME techniques (informatique, télécommunication…) et les PME non techniques. Les PME les plus sensibles à la confidentialité des données ainsi que celles qui dépendent fortement de la disponibilité et de l'intégrité de leurs informations.	Dagorn et Poussing (2012) ; Barlette (2012) ; -Cadre conceptuel holistique de Dojkovski (2007)
	Facteurs endogènes	La gestion des risques	C'est l'analyse et l'évaluation des risques liés au SI de l'entreprise et ensuite la mise en place des mesures pour contrer ces risques.	- Modèle holistique de la CSSI de Tolah et al (2017) -Théorie gouvernance des systèmes d'information (GSI) -Cadre conceptuel holistique de Dojkovski (2007)
		Réalisation d'actions de formation/ sensibilisation	La sensibilisation est l'amélioration de l'importance de la sécurité des systèmes d'information. La formation c'est un processus d'apprentissage qui fournit des connaissances générales sur un certain sujet lié à l'environnement de sécurité du SI et les compétences de requises pour que les employés exécutent les procédures de sécurité.	-Modèle de la CSSI d'Alnatheer et al (2012) - Modèle holistique de la CSSI de Tolah et al (2017) - Modèle de la CSSI de Martins et Da Veiga (2015) - Cadre conceptuel holistique de Dojkovski (2007)
	La direction	La sensibilité du dirigeant à la sécurité	Le degré de la compréhension par la haute direction de l'importance de la fonction de sécurité du SI et participe aux activités de sécurité visant à améliorer et à créer une forte culture de la SSI.	-Modèle de la CSSI d'Alnatheer et al (2012) - Modèle holistique de la CSSI de Tolah et al (2017) - Modèle de la CSSI de Martins et Da Veiga (2015)

La culture sécurité	Conscience de sécurité	Lorsque les utilisateurs comprennent les problèmes potentiels liés à la SSI et prennent conscience de l'importance de leur rôle en matière de sécurité.	-Modèle de la CSSI d'Alnatheer et al (2012) - Modèle holistique de la CSSI de Tolah et al (2017) - Modèle des trois niveaux de la culture de Schein (1985)
	Propriété de sécurité	La façon dont les employés perçoivent leurs responsabilités, leurs rôles et leur volonté d'agir de manière constructive pour améliorer leurs propres performances en matière de sécurité et celles de l'organisation.	-Modèle de la CSSI d'Alnatheer et al (2012) - Modèle holistique de la CSSI de Tolah et al (2017) - Modèle des trois niveaux de la culture de Schein (1985)
	Conformité à la sécurité	La connaissance par le personnel de la politique et des procédures de sécurité. Des faits visibles mais non encore interprétés, ça veut dire que cette conformité va se traduire par des comportements de sécurité si l'employé passe de l'intention de comportement à un comportement effectif.	- Modèle holistique de la CSSI de Tolah et al (2017) - Modèle des trois niveaux de la culture de Schein (1985) - Modèle de la CSSI de Martins et Da Veiga (2015)
Comportement lié à la sécurité	Comportement lié à la sécurité de l'utilisateur du SI	C'est le degré d'engagement des utilisateurs dans la SSI qui se manifeste par des comportements de sécurité effectifs (visibles).	Pérès et Latour (2000) ; Yves Barlette (2006) ; Parsons et al (2014).

Tableau 20 : Synthèse des concepts du modèle et leur origine

Synthèse de la section 1

Tout au long de cette section, nous avons défini les concepts mobilisés dans la construction de notre modèle conceptuel, et qui sont répartis en trois niveaux. Le premier niveau qui représente les facteurs qui influencent la culture sécurité, le deuxième niveau pour les composants de la culture sécurité et le dernier niveau pour les comportements liés à la sécurité. Pour définir le deuxième niveau, nous nous sommes basés sur le modèle de trois niveaux de culture de (Schein, 1985).

Section 2 : Modèle conceptuel et orientations de la recherche

Le but de cette section est de présenter en premier lieu, la structure générale de notre modèle conceptuel et en deuxième lieu, une description plus détaillée de ce modèle, et enfin les orientations de la recherche liées à ce modèle.

1. L'approche systémique

Notre recherche s'intéresse tout naturellement à l'homme (l'utilisateur), le système d'information (Système), les décisions qui concernent la sécurité des SI (Décideurs) et l'environnement, l'interaction entre ces trois éléments et leur environnement est présentée dans le schéma 1. La sécurité des systèmes d'information met en jeu des problématiques organisationnelles, qui sont de nature complexe (Morin, 1990; Genelot, 1998), et des problématiques humaines qui sont liées à une « hypercomplexité » (Morin, 1990).

Pour Reix (2004) : « *la question de la sécurité est un problème de gestionnaires et non un problème de spécialistes. (…) Sans réflexion organisationnelle, sans sensibilisation et formation des individus, elle risque de ne constituer qu'un investissement décevant; elle ne réussit qu'à travers une modification des attitudes et des comportements* ».

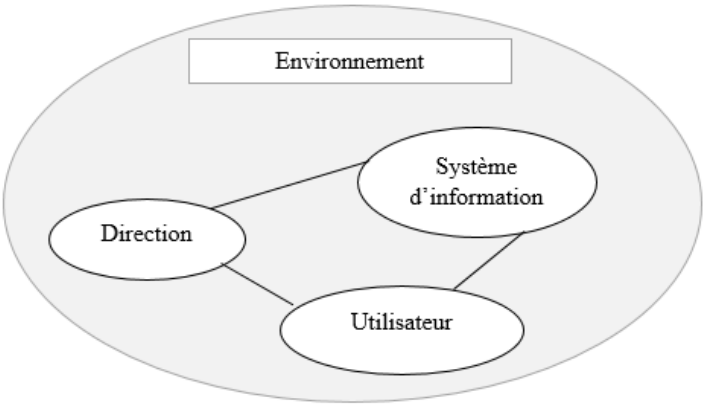


Figure 26 : Interaction homme-système-environnement

Notre recherche s'inscrit dans la logique de l'approche systémique qui se distingue des autres approches par sa façon de comprendre les relations humaines où l'individu fait partie et est influencé par différents systèmes : professionnel, social, familial… Les personnes dépendent les unes des autres et leurs échanges se font selon des règles implicites de communication

utilisées le plus souvent de manière inconsciente. L'approche systémique prend en compte la communication et les interactions entre les individus.

Von Bertalanffy propose les fondements de la systémique, dans « La théorie générale des systèmes » en formalisant le concept de système comme *« un ensemble d'unités en interactions mutuelles* ». Il approuve que les véritables systèmes sont ouverts et qu'ils interagissent avec leur environnement. Les systèmes peuvent ainsi acquérir de nouvelles propriétés et s'inscrivent dans un cycle fonctionnel en perpétuelle évolution. L'interaction mutuelle des parties unitaires du système est intégrée au système qui forme alors un tout indissociable. Les systèmes deviennent des « *totalités dont les éléments, en interaction dynamique, constituent des ensembles ne pouvant être réduits à la somme de leurs parties* » (Von Bertalanffy, 1993).

Le développement de la théorie des systèmes et de l'analyse des systèmes a permis à la systémique de s'établir progressivement comme une véritable discipline. Daniel Durand s'est basé sur une définition très exhaustive proposée en 1985 par le collège français de la systémique (Cf. Figure 2) pour décrire sous forme de graphique l'articulation et le périmètre de cette discipline (Durand, 2010) :

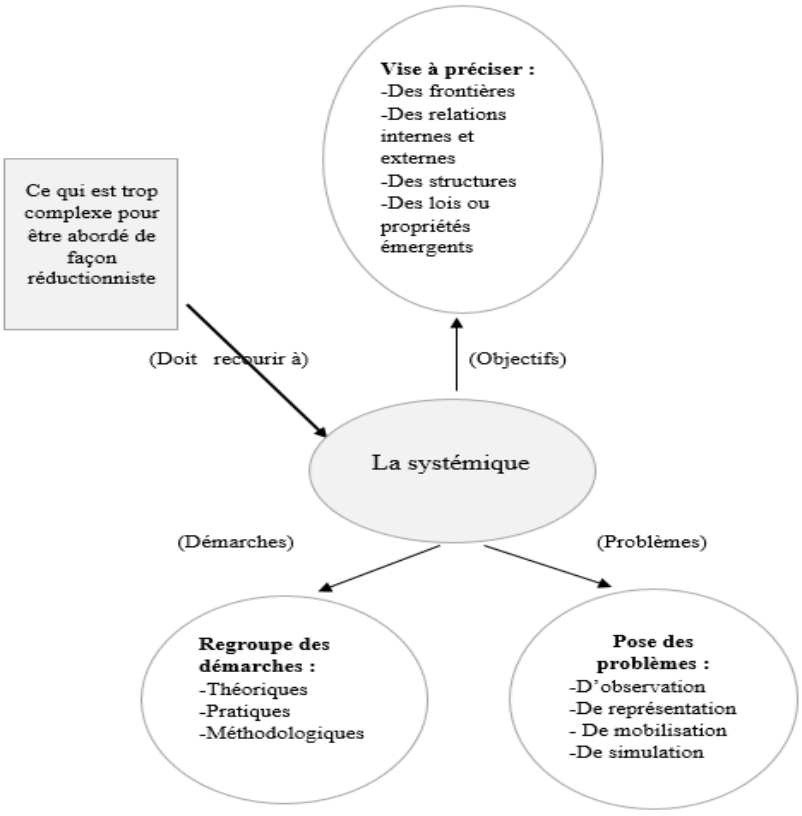


Figure 27 : La définition de la systémique du collège français (1985)
D'après (Durand 2010)

L’approche systémique de l’entreprise est ainsi considérée comme une discipline à part entière depuis les années 1980 (Zwingelstein, 1996): « *elle consiste à identifier et à modéliser toutes les interactions entre l’outil de production technique et des facteurs internes ou externes à l’entreprise* ». Notre recherche s’intéresse à l’interaction entre le système d’information, l’utilisateur, les décideurs et l’environnement dans le but d’étudier les multiples facettes de la culture sécurité.

Selon D. Genelot (1998, p111) et J.L Le Moigne (1995) : « *Pour comprendre un système compliqué, on peut le simplifier pour découvrir son intelligibilité (son explication). Pour comprendre et donner du sens à un système complexe, on doit le modéliser pour construire son intelligibilité (sa compréhension). Mais en simplifiant un système complexe, on le mutile et on détruit a priori son intelligibilité.* ». Notre objectif est de comprendre un système complexe, donc nous devons le simplifier à travers une modélisation. Cette modélisation sera une construction de l'esprit, donc subjective. (Le Moigne, 1995).

Nous étudions en particulier la culture sécurité des systèmes d’information, une approche qui va nous permettre de mieux comprendre les problématiques liées à la sécurité des systèmes d'information en PME. Nous visons donc à mieux comprendre cette culture et d’identifier les principaux leviers d’actions. Nous avons identifié l’intérêt de modéliser la situation de la culture sécurité des SI au sein de la PME vu sa complexité. Nous avons conçu un modèle (Figure X) que nous allons développer sa structure ci-dessous.

2. Présentation générale du modèle

Notre modèle conceptuel se décline du cadre théorique, et des analyses fondamentales qui s’inscrivent dans la perspective de la détermination des facteurs qui influencent et des facteurs qui constituent la culture sécurité de l’utilisateur des SI au sein de la PME.

Le modèle conceptuel fait état de trois niveaux d’analyse, concernant en premier lieu, des facteurs influençant la culture sécurité, en deuxième lieu, les composants d’une culture sécurité et en troisième lieu, les comportements liés à la sécurité. Le modèle conceptuel qui émerge (Figure 28), postule la relation entre ces trois niveaux.

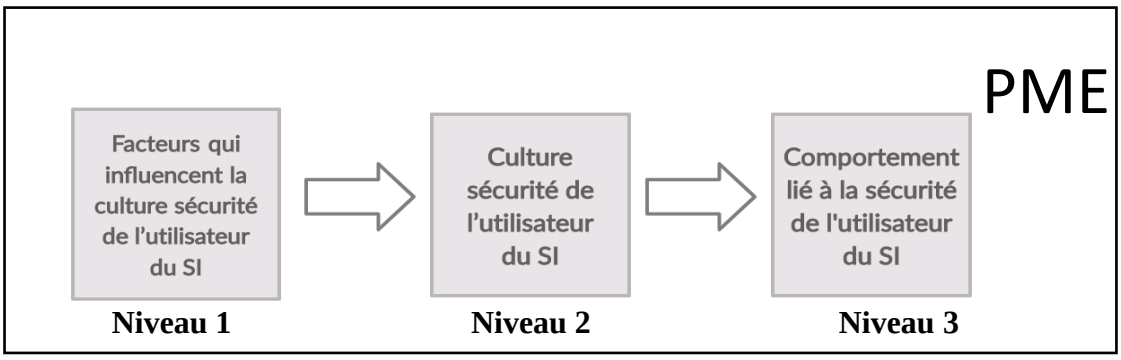


Figure 28 : Structure générale du modèle conceptuel

- **Le niveau 1 (*Input*) :** Représente les facteurs qui influencent la culture sécurité d'un utilisateur du SI, ces facteurs sont classés en facteurs exogènes émanant du contexte externe à l'entreprise, en facteurs endogènes qui se trouvent au sein de l'entreprise et enfin la direction qui est un facteur endogène mais que nous traitons à part vue sa spécificité et son importance.

- **Le niveau 2 (*Outcome*) :** Ce niveau concerne les déterminants d'une culture sécurité d'un utilisateur du SI, qui est impacté par le niveau 1.

- **Le niveau 3 (*Output*) :** Ce troisième niveau du modèle représente les comportements liés à la sécurité effectuée par l'utilisateur du SI. Ce niveau est le résultat du niveau 2 qui est la culture sécurité.

Ce modèle est destiné à être mis à l'épreuve de données acquises sur un terrain de recherche propice à conduire une étude empirique auprès des utilisateurs des SI. La présentation du terrain de recherche est détaillée dans le chapitre méthodologique suivant.

3. Description du modèle conceptuel

La structure de notre modèle résume les concepts mis en évidence par les travaux analysés dans le chapitre précédent. Ayant fait le choix de jauger la culture sécurité avec une finalité d'optimisation des comportements liés à la sécurité des utilisateurs des SI, le modèle conceptuel inclut, en se référant à la littérature, des construits, structurés en trois niveaux d'analyse, afférents aux facteurs qui influencent la culture sécurité, les facteurs qui constituent la culture sécurité et les comportements liés à la sécurité des utilisateurs (Figure 29).

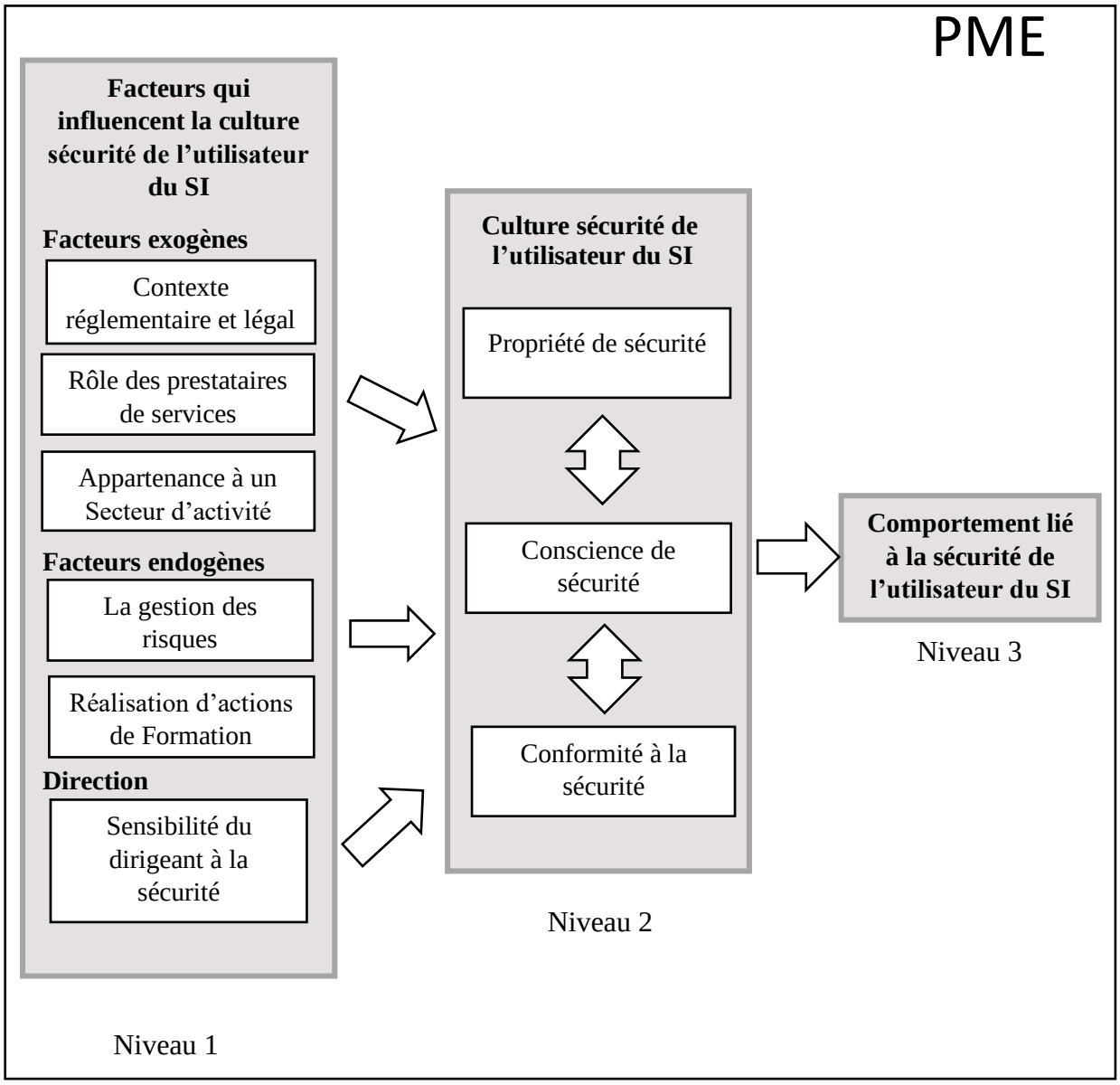


Figure 29 : le modèle conceptuel de la recherche

Le niveau (1) du modèle conceptuel

Ce niveau fait état des facteurs qui influencent la culture sécurité des utilisateurs des SI. Six facteurs divisés en trois catégories sont identifiés :

- **Facteurs exogènes**

- Contexte réglementaire et légal
- Rôle des prestataires informatiques
- Appartenance à un Secteur d'activité

- **Facteurs endogènes**

- La gestion des risques
- Réalisation d'actions de formation/sensibilisation

- **La direction**

- La sensibilité du dirigeant à la sécurité

Le niveau (2) du modèle conceptuel

Ce niveau fait état des composants d'une culture sécurité des utilisateurs des SI. Grâce à ces composants, nous pouvons déterminer le niveau de la culture sécurité. Trois composants sont identifiés :

- La conscience de sécurité
- Propriété de sécurité
- Conformité à la sécurité

Le niveau (3) du modèle conceptuel

Ce troisième niveau représente les comportements de sécurité des utilisateurs des SI. Ce niveau est la conséquence du deuxième niveau (La culture sécurité).

4. Les orientations de la recherche

Afin de comprendre la culture sécurité, ses déterminants et la relation avec les comportements des utilisateurs des SI, nous allons présenter nos orientations de recherche résultant de notre modèle conceptuel.

Orientation 1 : Les facteurs exogènes

Des facteurs exogènes comme le contexte légal ou la présence d'un prestataire informatique ou l'appartenance à un secteur d'activité sensible à la sécurité (Niveau 1) influencent positivement la culture sécurité SI (Niveau 2) de la PME. Dans cette étape nous étudierons le rôle et

l'influence exercés par des facteurs exogènes à la PME (le contexte réglementaire et légal, le prestataire informatique et le secteur d'activité) sur la culture sécurité des utilisateurs du SI.

Orientation 2 : Les facteurs endogènes

Des facteurs endogènes comme l'existence d'une évaluation des risques liés à la sécurité des SI ou la réalisation de formations en matière de sécurité des SI (Niveau 1) influencent positivement la culture sécurité SI de la PME (Niveau 2). Dans cette partie nous souhaitons montrer, dans un premier lieu, que la mise en place d'une gestion efficace des risques liés aux SI peut augmenter le niveau de sécurité du SI dans la PME ainsi que la culture sécurité des utilisateurs. Dans un deuxième lieu, le recourt à la formation et la sensibilisation des utilisateurs améliore leur culture sécurité.

Orientation 3 : La sensibilité de la direction à la sécurité

La direction de la PME (Niveau 1) joue un rôle important dans l'amélioration de la culture sécurité des utilisateurs du SI (Niveau 2). Le dirigeant de la PME joue un rôle essentiel dans la protection des SI, au travers des actions qu'il peut mettre en œuvre ou l'influence qu'il a sur ses employés. Si le dirigeant est impliqué dans la sécurité du SI de son entreprise il peut influencer l'implication de ses salariés et en conséquence, ça augmente leur cultures sécurité.

Orientation 4 : Relation culture-comportements

L'adoption d'une culture sécurité (Niveau 2) est favorable à créer un comportement lié à la sécurité (Niveau 3). Nous étudions dans cette partie, la relation entre la culture et le comportement, comment une forte culture de sécurité peut amener l'utilisateur du SI à adopter des comportements de sécurité tels que l'utilisation des mots de passe robustes difficiles à retrouver et difficiles à deviner, effectuer des sauvegardes régulières, contrôler la diffusion d'informations personnelles et des données de l'entreprise etc.

Synthèse de la section 2 :

Notre modèle théorique se compose des facteurs qui influencent la culture sécurité de l'utilisateur des SI qui sont à leur tour divisés en facteurs exogènes, des facteurs endogènes et la direction de la PME. La culture sécurité se compose de la propriété de sécurité, la conscience de sécurité et la conformité à la sécurité. Et enfin, si cette culture de sécurité est positive, elle

va influencer les comportements des utilisateurs pour protéger le SI de la PME. Dans cette section, nous avons présenté nos orientations de recherche postulant les relations entre les concepts de notre modèle conceptuel à savoir la relation entre les facteurs exogènes, les facteurs endogènes, la direction et la culture sécurité des utilisateurs. Et enfin la relation entre la culture sécurité et les comportements liés à la sécurité. Après la construction de notre modèle théorique et la présentation de nos orientations de recherche, il s'agit maintenant d'aller identifier sur le terrain des indices permettant de mieux comprendre quels sont les facteurs qui influencent la culture sécurité des utilisateurs du SI et quelles conséquences sur les comportements de ces utilisateurs afin de protéger le SI, et ce qui pourrait permettre d'améliorer la culture ainsi que les comportements des utilisateurs.

Conclusion du chapitre 2

L'objectif de ce deuxième chapitre était de développer un modèle conceptuel qui permet de répondre à la question de recherche : « *Comment insuffler une culture sécurité des systèmes d'information en PME ?* ». Pour cela, une démarche mettant en œuvre à la fois la revue de la littérature effectuée dans le premier chapitre et les spécificités du terrain de recherche a été adoptée. Les travaux de recherches conduits sur la culture sécurité des SI ont servi de support pour concevoir un modèle d'évaluation de la culture sécurité des SI dans la PME. Ce modèle comporte trois niveaux qui concernent les facteurs qui influencent la culture sécurité de l'utilisateur des SI (Niveau 1), la culture de sécurité de l'utilisateur du SI (niveau 2) et enfin les comportements des utilisateurs liés à la sécurité du SI (niveau 3). La particularité du modèle proposé se rapporte au fait qu'il est adapté à l'environnement de la PME d'une part, et d'une autre part, qu'il propose les facteurs qui influencent la culture sécurité, les facteurs qui composent cette culture et la relation entre culture et comportement. Les relations entre les trois niveaux du modèle sont expliquées sous forme d'orientations de recherche qui vont être examinées à partir de notre terrain de recherche. Dans la deuxième partie, nous allons donc chercher à explorer les orientations liées à notre modèle de recherche. Tout d'abord, nous traiterons de la méthodologie à mettre en place et ensuite les orientations confrontées à nos résultats issus du terrain. Après avoir discuté ces résultats en regard avec les éléments théoriques, nous en tirerons les principales conclusions, apports et limites.

Conclusion de la première partie

Nous avons développé au niveau de cette partie les concepts utiles à notre thèse. Dans un premier temps, nous avons proposé une définition de ce qu'est une culture sécurité des SI (CSSI), puis nous avons analysé les théories et les modèles qui concernent la CSSI, pour pouvoir en extraire les facteurs qui peuvent jouer un rôle sur la CSSI. Nous avons aussi étudié la relation entre CSSI et les comportements relatifs à la SSI. Ensuite, un ensemble d'actions à mettre en place pour sécuriser un SI d'une organisation a été proposé.

Dans un deuxième temps, nous avons pu construire un modèle conceptuel à partir de l'analyse de la littérature sur la CSSI, ce modèle est composé de trois niveaux, le premier concerne les facteurs qui influencent la CSSI, le deuxième représente les facteurs qui composent la CSSI et le troisième, c'est le résultat des deux premiers et qui est le comportement lié à la SSI. À ce modèle, nous avons associé quatre orientations de recherche. Les trois premières concernent la relation entre les deux premiers niveaux du modèle et la dernière concerne la relation entre le deuxième et le troisième niveau du modèle.

L'objet de la partie suivante est alors d'observer empiriquement le bien-fondé ou non de notre cadre conceptuel, de vérifier chacune de nos orientations de recherche à travers notre étude terrain et l'analyse des résultats qui en résulte.

Partie II
Déploiement du modèle conceptuel de la culture sécurité : Méthodologie et résultats

La première partie de notre thèse nous a aidé à mieux cerner le contexte au sein duquel évolue la culture sécurité des SI, nous permettant dès lors de construire un modèle théorique relatif à la culture sécurité des SI dans la PME, avec les facteurs agissant sur cette culture. La question de recherche étant désormais clairement posée, notre seconde partie s'attache à y répondre. A cette fin, étant donné que nous commençons à alterner réflexions théoriques et études empiriques, nous présentons tout d'abord le positionnement épistémologique ainsi que la méthodologie déployée, afin de clarifier la démarche générale. Nous examinons par la suite les modalités de notre modèle de la culture sécurité par le biais d'une étude qualitative menée auprès de huit PME, afin de déterminer les caractéristiques de ce que nous appelons la culture sécurité des SI **(chapitre 3)**. Les résultats de l'étude menée sont enfin discutés et un modèle théorique issu de cette étude sera présenté **(chapitre 4)**.

Figure 30 : Plan de la recherche (Partie II)

Introduction générale

Chapitre préliminaire : L'intentionnalité de la recherche

Partie I :

Conception d'une culture sécurité des SI en PME : vers un modèle conceptuel

Chapitre 1 : La culture sécurité des systèmes d'information dans les PME: Une revue de littérature

1) Etat des lieux de la connaissance
2) Les comportements liés à la sécurité
3) Les mesures de sécurité

Chapitre 2 : Construction d'un modèle théorique adapté à la PME et orientations de recherche

1) Précisions des concepts du modèle
2) Modèle conceptuel et orientations de la recherche

Partie II :
Déploiement du modèle théorique de la culture sécurité: Méthodologie et résultats

Chapitre 3 : Etudes de cas: pratiques des PME en sécurité des SI

1) Positionnement épistémologique et méthodologie
2) Vers une typologie des cas étudiés : analyse des résultats

Chapitre 4 : Examen des orientations de recherche et discussion des résultats

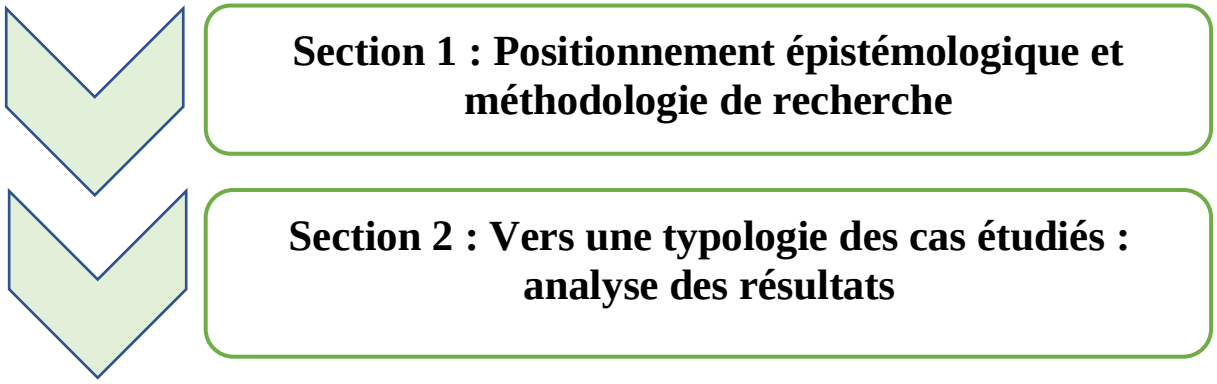
1) Retour sur les orientations de recherche et discussion des résultats
2) Retour sur le modèle conceptuel

Conclusion générale

Chapitre 3

Etudes de cas : les pratiques des PME en sécurité des SI

Le présent chapitre vise à expliciter le positionnement épistémologique retenu, ici en l'occurrence le positivisme, puisque nous nous inscrivons dans une approche qui vise à comprendre la réalité. Ensuite, après la présentation de notre type de raisonnement à savoir le raisonnement abductif, nous exposons notre méthodologie qualitative mise en place **(Section 1)**. Après la discussion du positionnement épistémologique et de la méthodologie de recherche, nous présentons les principaux résultats de notre étude des cas réalisée au sein de huit PME en proposant une typologie de ces cas étudiés **(Section 2)**.



Section 1 : Positionnement épistémologique et méthodologie de recherche

Selon Piaget (1967), l'épistémologie est définie comme l'étude de la constitution des connaissances valables. Dans sa considération la plus ancienne, l'épistémologie désigne de manière relativement large l'étude de la connaissance scientifique. Plus précisément, il s'agit d'une branche de la philosophie ayant pour objet d'étudier et de porter un regard critique sur les postulats et méthodologies au sein d'une science particulière afin d'en déterminer la valeur et la crédibilité scientifique. Dans cette section, nous allons présenter notre positionnement épistémologique, notre raisonnement de recherche et notre méthodologie de recherche.

1. Un positionnement épistémologique interprétativiste

Le positionnement épistémologique consiste à opérer le choix du paradigme et de la méthode pour conduire la recherche. Classiquement, il existe trois paradigmes épistémologiques : le positivisme, l'interprétativiste et le constructivisme (Girod-Séville et Perret ; 1999). Parmi ces paradigmes lequel semble le plus convenable pour répondre à nos questions de recherche ?

Avant de répondre à cette question, nous rappelons les définitions de ces trois paradigmes :

-Le **paradigme positiviste**, sa finalité consiste à expliquer la réalité et considère des hypothèses plutôt déterministes. Le paradigme positiviste est fréquemment exposé comme celui dominant les sciences de l'organisation et postule un positionnement réaliste (Thiétart et al. 2003). Le chercheur est amené à extirper sa « subjectivité » face à la réalité empirique (Thiétart et al. 2003). Avison et Myers (2002) postulent dans ce sens que « *les positivistes estiment généralement que la réalité est objectivement donnée et qu'elle peut être décrite par des propriétés mesurables qui sont indépendantes de l'observateur (le chercheur), ainsi que de ses instruments* ».

-Le **paradigme constructiviste**, est basé sur l'acceptation d'un univers construit avec les représentations des acteurs. C'est ce qui nécessite des qualités et des aptitudes d'observation, d'écoute et de questionnement qui permettent d'accéder à une certaine maîtrise des éventuels biais cognitifs qui pourraient retenir un chercheur (Girod-Séville et Perret ; 1999). Ce

paradigme a pour objet la construction de la réalité (Le Moigne, 1994 ; Thiétart et al. 2003). Et il soutient que la compréhension participe à la construction de la réalité des acteurs étudiés. Cette position constructiviste est produite par le chercheur à parti, et d'après sa propre expérience et dans son propre contexte expérimental (Girod-Séville et Perret, 1999).

-Le **paradigme interprétativiste**, selon la littérature, cette approche est classifiée comme une approche médiatrice. Elle s'oppose en partie au positivisme et partage avec le constructivisme quelques postulats. Dans les limites de l'interprétativiste, la voie de la connaissance scientifique est celle de la compréhension alors que la construction est favorisée dans le constructivisme (Girod-Séville et Perret, 1999). Dans ces deux derniers paradigmes, il est approuvé que la connaissance produite est contextuelle, mais le plus souvent l'interprétativiste prospecte la compréhension tandis que le constructivisme s'inscrit dans une démarche plus pragmatiste (Trauth et Jessup, 2000).

Le courant interprétativiste vise à comprendre la réalité, non à l'expliquer (positivisme), ni à la construire (constructivisme). Pour les interprétativistes, « *La réalité ne sera jamais indépendante de l'esprit, de la conscience de celui qui observe ou l'expérimente* » (Girod-Séville et Perret, 1999, p. 19). La réalité dépend donc de l'observateur.

Dans le domaine des S.I., le courant interprétativiste considère que « *Le S.I. n'existe pas indépendamment de l'observateur* » (Rowe, 2002) et que les méthodes de recherche interprétativistes sont « *Destinées à produire une compréhension du contexte des systèmes d'information* » (Walsham, 1993, p. 4).

Dès lors, nous inscrivons pour notre part nos travaux de recherche dans le cadre d'un paradigme épistémologique interprétativiste, dans la mesure où :

-Nous cherchons à mieux comprendre la culture et les comportements liés à la sécurité des systèmes d'information.

-Il n'existe pas une réalité qui soit unique, mais bien une pluralité de réalités qui sont fonction de l'expérience vécue par les acteurs. Ces multiples réalités précèdent la connaissance.

-Nous cherchons, via notre interprétation, à nous représenter de la manière la plus fidèle possible la manière dont les acteurs (dirigeants, responsables et utilisateurs) perçoivent et reflètent la sécurité des SI.

-Il existe une interdépendance entre le réel et l'observateur tout comme entre le chercheur et l'objet de l'étude.

Nous allons aborder ensuite, le raisonnement de notre recherche et la méthodologie de l'étude qualitative déployée.

2. Une démarche abductive

Au cours de notre recherche, nous avons adopté un mode de raisonnement de type abductif. Selon Koenig (1993) : « *L'abduction est l'opération qui, n'appartenant pas à la logique, permet d'échapper à la perception chaotique que l'on a du monde réel par un essai de conjecture sur les relations qu'entretiennent effectivement les choses […]. L'abduction consiste à tirer de l'observation des conjectures qu'il convient ensuite de tester et de discuter* ».

Nous ne prétendons pas dégager une théorie définitive concernant la culture sécurité. Notre recherche est donc bien plus guidée par la volonté d'explorer que de tester. En procédant par abduction, nous comptons aborder le phénomène à étudier avec un minimum d'idées préconçues afin d'explorer le terrain, autrement dit, en essayant de nous rendre le plus possible réceptif à la réalité qui émerge de nos observations et puis seulement dans un deuxième temps, à conceptualiser les différents matériaux récoltés (Beaud et Weber, 1998).

Dans les recherches en management, les méthodes exploratoires sont communément utilisées dans le but de concevoir de nouveaux appareils théoriques plutôt que pour les tester (Snow et Thomas, 1994). Notre raisonnement abductif se dessine de cette manière par une exploration hybride entre exploration théorique et empirique (Thietart et al. 2014). Hybride dans la mesure où nous explorons dans un premier temps un phénomène en partant principalement d'un terrain de recherche et en se basant ensuite sur les théories en lien avec le phénomène étudié. Nous nous attachons ainsi à enrichir des connaissances antérieures « *en procédant par allers retours fréquents entre le matériau empirique recueilli et la théorie* » (Thietart et al. 2014). La démarche abductive peut être considérée comme un jeu d'allers et retours entre théorie et terrain au sein duquel « *il s'agit bien de confronter des schémas théoriques à des observations réalisées en situations réelle et pour lesquelles le chercheur ne peut avoir une place d'observateur neutre, dans la mesure où les acteurs vont lui affecter un rôle dans le processus* » (Girin, 1990).

Si le chercheur n'a pas l'obligation de tester les résultats finaux obtenus, il s'agit tout de même de « *formuler le cadre théorique nouveau de manière à ce qu'il soit testable par la suite sur*

d'autres terrains de recherche que celui ou ceux qui ont été précédemment utilisés » (Thietart et al. 2014). Notre démarche abductive s'inscrit dans une approche exploratoire dans la mesure où nous partons en grande partie du terrain et que la revue de littérature théorique issue de nos premières observations empiriques ne débouche pas sur la formulation d'hypothèses mais plutôt sur la construction d'un cadre conceptuel dont il s'agit de tester les conjectures/modalités.

3. Méthodologie de l'étude qualitative

3.1 Objectifs de l'étude qualitative

La recherche qualitative est caractérisée par une évaluation en profondeur des motivations et des freins au développement d'une culture sécurité des SI. Elle permet d'expliquer les mécanismes psychologiques qui peuvent former la culture sécurité des SI de l'utilisateur.

L'objet d'une recherche qualitative est d'étudier un phénomène humain qui n'est pas directement visible, avec deux objectifs : d'un côté, sa compréhension, c'est-à-dire connaître le « comment » du phénomène et d'un autre côté, se donner une possibilité d'agir sur le phénomène ou la situation dans laquelle il se trouve. C'est ainsi que le chercheur observe plus particulièrement « les comportements, les histoires de vie, les interactions sociales, les fonctionnements organisationnels ou les mouvements sociaux » (Wacheux, 1996).

Les données qualitatives soulignent ainsi l'importance du contexte, des personnes et des issues individuelles et ainsi, fournissent une compréhension plus profonde de ce qui se produit réellement. C'est ce qui éclaircit l'intérêt d'une telle approche pour cette recherche, étant donné que nous essayons de comprendre la réalité en profondeur, telle que perçue par les acteurs.

Généralement, la recherche qualitative est exécutée auprès de groupes de répondants significativement plus réduits que dans le cas des recherches quantitatives (Igalens et Roussel, 1998), et cela, afin de recueillir des informations signifiantes et en profondeur concernant les différents aspects du comportement de l'interviewé.

L'approche qualitative retenue repose sur des entretiens semis directifs qui ont été suivis par des analyses de contenu. La démarche suivie se base sur un basculement entre la revue de la littérature et l'analyse de contenu. Ce processus, fait d'allers/retours montre la nécessité d'intégrer les nouvelles découvertes du terrain aux réflexions conduites dans la démarche théorique. En effet, si le suivi d'une démarche d'allers et de retours entre la théorie et la pratique

est indissociable d'une démarche méthodologique de nature qualitative, elle est également le garant d'une plus grande proximité entre la réflexion et les faits (Girod-Séville et Perret ; 1999).

Cette approche qualitative nous a permis de vérifier l'existence des caractéristiques identifiées par le cadre théorique, d'explorer le terrain d'investigation, d'en repérer. Deux objectifs ont donc été liés à cette étude qualitative :

- Le premier est de nature confirmatoire, il consiste à s'assurer que les principaux critères mentionnés dans la revue de littérature sont approuvés dans les verbalisations des interviewés ;
- Le second est de nature exploratoire, il vise l'enrichissement des conclusions de la littérature par la production de nouvelles informations.

3.2 La méthode qualitative mobilisée

Pour réaliser une recherche avec des méthodes qualitatives, le chercheur peut se référer à plusieurs stratégies de recherches. Yin (1994) identifie l'expérimentation, l'étude de cas, l'enquête, l'étude historique et l'analyse des archives. Le tableau suivant présente une comparaison entre ces différentes stratégies :

Stratégie	Forme de la question de recherche	Contrôle sur des évènements comportementaux	Focus sur les évènements contemporains
Expérimentation	Comment, pourquoi	Oui	Oui
Enquête	Qui, quoi, où, combien	Non	Oui
Analyse des archives	Qui, quoi, où, combien	Non	Oui/Non
Etude historique	Comment, pourquoi	Non	Non
Etude de cas	Comment, pourquoi	Non	Oui

Tableau 21 : Comparaison des différentes stratégies de recherche qualitatives D'après Yin (1994)

Nous avons fait recours à la stratégie d'étude de cas, puisque notre question de recherche principale est de type : « comment ». Nous allons détailler ce choix dans l'élément suivant.

3.2.1 L'étude de cas

Del Bayle (2000) révèle que la technique de l'étude de cas « *a été mise au point dans la seconde moitié du XIXe siècle par le sociologue français Le Play (1806-1882) qui l'a utilisée afin d'étudier les problèmes sociaux nés du développement de la société industrielle à travers l'analyse monographique de familles ouvrières appartenant à différents pays européens* ».

Aujourd'hui, l'étude de cas est largement reconnue comme stratégie de recherche en sciences de gestion. Stake (2005) affirme que cette méthodologie est devenue l'une des méthodes les plus utilisées pour mener des études qualitatives. Plusieurs travaux de référence ont participé à établir sa légitimité (Eisenhardt 1989 ; Yin 1994 ; Yin 2003 ; Guba & Lincoln 1994). Ces travaux ont mis en évidence son intérêt scientifique et ont fourni des techniques et des méthodes d'investigation spécifiques afin d'améliorer sa validité.

L'étude de cas est considérée comme l'étude approfondie d'un objet de recherche, ce qui permet d'obtenir une connaissance vaste et détaillée de ce dernier. L'idée principale de l'étude de cas est que si nous étudions avec attention toute unité d'un certain univers, nous serons dans les conditions de connaître quelques aspects généraux de celui-ci.

Notre objet de recherche a été peu étudié jusqu'à présent, ce qui justifie l'adoption de cette méthode (Yin, 1984 ; Eisenhardt, 1989). D'autre part, dans notre démarche de compréhension de la culture sécurité, nous avons déjà identifié un cadre théorique ce qui renforce l'intérêt d'adopter une démarche d'étude de cas (Igalens et Roussel, 1998).

Yin (1994) définit la méthode de recherche d'étude de cas comme « *une enquête empirique qui étudie un phénomène contemporain dans son contexte réel ; quand les frontières entre le phénomène et le contexte ne sont pas clairement évidentes ; et dans lesquelles de multiples sources d'évidences sont employées ; et en bénéficiant des précédents développements théoriques pour la collecte et l'analyse des données* ».

La méthode de l'étude de cas est difficile à réaliser (Yin 1994). Le chercheur doit mener son étude rigoureusement afin de s'assurer de la validité des connaissances produites. La validité d'une recherche est définie par Wacheux (1996) comme «*la capacité des instruments à apprécier effectivement et réellement l'objet de la recherche pour lequel ils ont été créés* ». Yin

(1994) a classifié quatre types de validité : la validité du construit, la validité interne, la validité externe et la fiabilité.

La validité du construit exige du chercheur d'employer les mesures opérationnelles correctes pour les concepts étudiés. La validité interne démontre que certaines conditions mènent à d'autres et donc exige l'utilisation de preuves et de sources multiples. Quant à la validité externe, elle reflète si les résultats sont généralisables. Enfin, la fiabilité se rapporte à l'exactitude, à la stabilité et à la précision de la mesure. La conception exemplaire de l'étude de cas s'assure que les procédures utilisées sont bien documentées et peuvent être répétées, à plusieurs reprises, avec les mêmes résultats (Yin 1994).

Yin (1994) propose de suivre un certain nombre de techniques durant la conception et la réalisation de l'étude de cas, dans le but de garantir sa validité. Ces techniques sont résumées dans le tableau suivant :

Tests	Technique	Phase de recherche D'application de la technique
Validité du construit	-Utiliser plusieurs sources d'évidence -Etablir une chaine d'évidences -Une revue par des informants clés du projet du rapport de l'étude de cas.	-Collecte de données -Collecte de données -Composition/rédaction
Validité interne	-Faire la correspondance des modèles -Faire la construction-explication -Réaliser des analyses sur les séries chronologiques.	-Analyse de données
Validité externe	-Faire de la réplication sur des cas multiples	-Design de recherche
Fiabilité	-Utiliser un protocole pour l'étude de cas -Développer une base de données pour l'étude de cas.	-Collecte de données -Collecte de données

Tableau 22 : Techniques pour l'étude de cas, (Yin, 1994)

Ces techniques ont pour objectif d'assurer la rigueur de l'approche et de produire des résultats valides. D'autant plus que l'étude de cas est généralement critiquée pour certaines limites, il est difficile de généraliser ses résultats (Yin 1994). Les chercheurs admettent que les résultats issus

de démarches d'étude de cas ne sont pas généralisables selon un raisonnement d'inférence statistique. David (2005) exprime que dans le cadre des études de cas, il y a lieu de parler de généralisation des propositions théoriques et non de généralisation aux populations et univers. Koenig (2005) affirme même que, d'un point de vue interprétativiste, la valeur d'un cas tient à ce qu'il a d'unique.

Un autre choix méthodologique s'impose : le choix d'étudier un cas unique ou des cas multiples. Yin (1994) distingue, en fonction du design, quatre types d'études de cas : étude de cas unique holistique, unique enchâssée, étude de cas multiples holistique ainsi qu'étude de cas multiples enchâssée. Le tableau 3 présente ces quatre types, le premier une étude de cas unique de type holistique basée sur une seule unité d'analyse ; le deuxième une étude de cas unique de type enchâssé (*Embedded*) investigue plusieurs unités d'analyses dans un seul cas ; le troisième une étude de cas multiples de type holistique qui étudie plusieurs cas et chacun comme une unité d'analyse ; et enfin, une étude de cas multiples de type enchâssé couvre plusieurs cas et chaque cas englobe un certain nombre d'unités d'analyse (Yin 1994).

	Cas unique	Cas multiples
Holistique (Une seule unité d'analyse)	Type 1	Type 3
Enchâssé (Unités d'analyse multiples)	Type 2	Type 4

Tableau 23 : Types de designs d'études de cas, adaptés de (Yin 1994)

Selon Yin (1994), le recours à l'étude cas unique se fait dans les situations suivantes : un cas critique pour tester une théorie déjà formulée, un cas extrême ou unique, un cas révélateur.

Gagnon (2012) affirme que l'étude de cas unique est recommandée pour une problématique de type empirique brut, c'est-à-dire un phénomène inexploré ou peu exploré. Il insiste sur le fait que cela ne veut pas dire que l'étude de cas unique n'est pas une unité d'analyse utile pour l'élaboration de certaines théories, en donnant l'exemple de plusieurs études relatives aux organisations et aux systèmes sociaux (Gagnon 2012).

Nous avons choisi de faire recours à l'étude de cas multiples de type enchâssé, et nous motivons ce choix dans le sous-titre suivant.

3.2.2 L'étude de cas multiples enchâssés

L'étude de cas multiples est une méthodologie fréquemment utilisée par les chercheurs qui réalisent des études comparatives, multipliant les points de vue et les cas afin de tendre vers une compréhension globale du phénomène. Selon Yin (2003), le recours à plusieurs cas augmente la force des preuves, la multiplication des exemples et points de vue est vecteur de variance et garantit une plus grande robustesse des résultats par rapport à l'étude de cas unique. Eisenhardt (1991) maintient l'intérêt de multiplier les cas, notamment lorsque l'objectif de la recherche est la généralisation des résultats. Hormis ses intérêts en terme généralisable, l'étude de cas multiples présente également l'avantage de réduire les biais liés à l'idiosyncrasie des résultats obtenus.

Notre recherche s'appuie sur une étude de cas multiples, de nature enchâssée. Ce choix se justifie par la nature hétérogène et la singularité de l'objet de recherche retenu, à savoir les PME. Dans une étude de cas de type enchâssé, le chercheur analyse plusieurs unités qui peuvent être, dans le cas d'une organisation, des structures, des projets, etc. L'intérêt d'un design enchâssé réside largement dans la possibilité d'analyser à la fois les différentes unités, le cas dans son ensemble et leurs interactions réciproques. La prise en compte de niveaux multiples permet au chercheur d'approfondir ses analyses pour essayer de comprendre les similitudes ou contrastes relevés. En ce sens, un design enchâssé peut aider à formuler des propositions sur des phénomènes qu'il aurait été difficile d'appréhender avec un design holistique.

Le chercheur peut sélectionner des unités qui lui paraissent offrir des éléments de contraste, tout en étant pertinentes par rapport à ses questions de recherche : projets dont la nature ou l'objectif sont différents, groupes de niveaux hiérarchiques contrastés, acteurs de métiers et fonctions divers. Il convient également de veiller lors de la sélection des unités d'analyse à la fréquence du recueil des données, à la durée de ce recueil et le degré de précision envisagé, selon les recommandations de Van de Ven et Poole (2002).

Nous avons choisi deux unités d'analyse principales à savoir la direction de la PME où nous investiguant la prise de décisions qui concerne la sécurité des SI et les facteurs qui influencent cette prise de décision. Et la deuxième unité d'analyse concerne les salariés de la PME qui représentent les utilisateurs des SI avec lesquels nous investiguant la maturité de la culture sécurité et les comportements liés à la sécurité. La figure suivante représente notre choix d'unités :

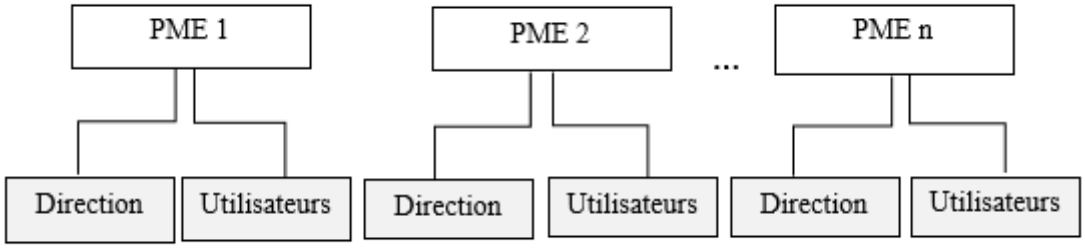


Figure 31 : La présentation d'unités d'analyse choisis dans le cadre de l'étude de cas multiples

4 La méthode de collecte de données

La collecte de données qualitatives peut se faire à travers plusieurs méthodes. Nous allons présenter les deux grandes familles, à savoir les entretiens et les techniques projectives. Les **techniques projectives** sont généralement considérées comme des « épreuves psychométriques » : l'expression apparaît en 1939 afin de « rendre compte de la parenté entre trois épreuves psychologiques : le test d'associations de mots de Jung (1904), le test des tâches d'encre de Rorschach (1940) ainsi que le test d'histoire à inventer de Murray (1935) » (Gavard-Perret et al, 2018).

Pour pallier les insuffisances des techniques directes de collecte de données (questionnaire ou entretien) dans l'exploration des motivations profondes d'un individu, de sa personnalité, ses valeurs, ses attitudes, etc. Les techniques projectives maintiennent à contourner le matériau conscient de l'individu pour dévoiler des raisons moins conscientes, mais plus révélatrices des véritables motifs sous-jacents d'un comportement. Le principe sous-jacent est celui de la projection présentée par Freud comme « *le processus par lequel le sujet expulse de soi et localise dans l'autre, personne ou chose, des qualités, des sentiments, des désirs, voire des ''objets'' qu'il méconnaît ou refuse en lui* ». (Laplanche et Pontalis, 1967).

En ce qui concerne **l'entretien,** c'est « *une des méthodes qualitatives les plus utilisées en sciences de gestion* », (Kahn et Cannell, 1957). Il peut être considéré comme « *une conversation avec un objectif* », (Gavard-Perret et al, 2018) ou encore « *un dispositif de face-à-face où un enquêteur a pour objectif de favoriser chez un enquêté la production d'un discours sur un thème défini dans le cadre d'une recherche* », (Freyssinet-Dominjon, 1997). Il existe deux formes d'entretien : le premier est l'entretien de groupe et le deuxième est l'entretien individuel.

L'entretien de groupe consiste à réunir, autour d'un animateur (le chercheur), un ensemble de personnes dans le but de les amener à interagir. Cette technique est basée sur la théorie de la dynamique des groupes restreints de Lewin (1952). En sciences de gestion, les entretiens de groupe sont utilisés pour susciter des idées, affiner un diagnostic ou la définition d'un problème, explorer des opinions, etc. L'entretien de groupe tire profit des interactions entre les membres interrogés et permet d'analyser les processus d'interrelations en action. « Le jeu des interactions et des influences réciproques élargit la réflexion et accroît la production scientifique ». (Pellemans, 1999).

Par ailleurs, il n'existe pas de consensus clair sur la catégorisation des entretiens de groupe. Certains auteurs ne comptent que quatre types : groupes de discussions, groupes de réflexion, groupes nominaux et groupes Delphi. D'autres comme Andreani (1998) et Albarello (2004) mentionnent des catégories supplémentaires : groupes de créativité, groupes d'experts, mini-groupes, groupes de motivation, groupes projectifs, etc.

Quant à **l'entretien individuel**, il est bien adapté pour l'exploration de processus individuels complexes (évaluation, compréhension, décision, immersion, etc.) ou de sujets confidentiels, touchant à l'intimité de l'individu ou encore tabous (la religion, le tabac, la mort, l'argent, etc.) et/ou pour mettre en évidence des différences individuelles. Gavard-Perret et Al, (2018) distinguent trois formes d'entretiens individuels en fonction du niveau de saturation de l'interaction entre l'enquêteur et l'individu : directif, semi-directif et non directif. Ces formes d'entretiens se caractérisent par des degrés croissants d'exploration en profondeur des représentations individuelles et, en parallèle, par des degrés décroissants d'intervention de l'enquêteur. La figure suivante représente les degrés d'exploration et d'intervention pour chaque forme d'entretien.

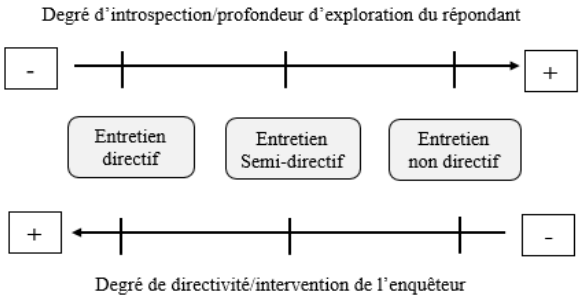


Figure 32 : Degré d'exploration et d'intervention adapté de (Gavard-Perret et al, 2018)

Ketele et Roegiers (1996) soulignent les caractéristiques de chaque type d'entretien (directif, semi-directif et non directif). Le tableau suivant présente synthétiquement les caractéristiques des trois types d'entretien.

Entretien directif (Ou dirigé)	Entretien semi-directif (Ou semi-dirigé)	Entretien non directif (Ou non dirigé)
Discours non continu qui suit l'ordre des questions posées	Discours par thèmes dont l'ordre peut être plus ou moins bien déterminé selon la réactivité de l'interviewé	Discours continu
Questions préparées à l'avance et posées dans un ordre bien précis	Quelques points de repère pour l'interviewer	Aucune question préparée à l'avance
Information partielle et réduite	Information de bonne qualité, orientée vers le but poursuivi	Information de très bonne qualité, mais pas nécessairement pertinente
Information recueillie rapidement ou très rapidement	Information recueillie dans un laps de temps raisonnable	Durée de recueil d'informations non prévisible
Inférence assez bien	Inférence modérée	Inférence exclusivement fonction du mode de recueil

Tableau 24 : Caractéristiques des trois types d'entretiens
D'après De Ketele et Roegiers (1996)

Churchill (1979) souligne la nécessité de mener des entretiens semi-directifs exploratoires afin d'augmenter la probabilité de produire des mesures valides. Evrard et al. (2003) qualifient l'entretien semi- directif comme le plus performant pour faire émerger les motivations et les attitudes. Certes, l'entretien de groupe est une autre mode de collecte intéressante, mais son choix dépend souvent de la nature du sujet à traiter : les thèmes à aborder sont facilités par la présence des autres, les attitudes et la consommation sont sujettes à des phénomènes d'influence de groupe (leadership professionnel, normes de prescriptions, etc.), sujets angoissants (assurance vie, sida, etc.) (Evrard et al, 2003). Afin de répondre aux objectifs visés par cette recherche, notre choix s'est porté sur les entretiens individuels semi-directifs. Ce choix est aussi motivé par le fait que l'utilisateur interagit avec le SI généralement de façon individuelle. Le recueil de données a consisté en des entretiens semi-directifs dont le principe, le déroulement et le profil des répondants, seront présentés ci-après.

5 Entretiens semi-directifs

L'entretien semi-directif : ce type d'entretien se situe entre l'entretien directif et non directif. Il se caractérise par le fait qu'il laisse à l'interviewé un espace assez large pour exprimer son point de vue. L'enquêteur pose des questions et laisse l'enquêté répondre en toute liberté. Le rôle de l'interviewer dans ce type d'entretien est d'encourager l'informateur à parler et donner davantage d'informations sur la thématique de sa recherche. Les questions posées dans ce type d'entretien sont relativement ouvertes. L'interviewer doit les recentrer afin de ne pas perdre de vue l'objectif qu'il s'est fixé (Blanchet et Gotman, 2010).

L'entretien semi-directif se déroule à partir d'un guide d'entretien qui reprend la liste des thèmes qui doivent être abordés au cours de l'entretien. Ces thèmes doivent être mis à jour par le chercheur, validés par un pré-test ou par un expert et sur lesquels on demande à la personne interviewée de s'exprimer (Igalens et Roussel, 1998, p. 79). Ils représentent des questions de recherche conceptualisées et traduites dans le langage des répondants (Wacheux, 1996, p. 206).

Ce guide doit permettre d'harmoniser le cadre et l'orientation des divers entretiens et garantir des conditions assez proches d'un entretien à l'autre, en conformité avec les principes de l'étude de cas multiples, qui exigent une certaine harmonie dans les données produites. Dans les sections suivantes, nous présentons le déroulement des entretiens, leurs analyses ainsi que les résultats de ces derniers.

5.2Le déroulement des entretiens semi-directifs

Cette étude s'est effectuée entre les mois de juillet 2019 et de mars 2020. Notre premier contact a été une entreprise qui a été victime d'une tentative de fraude dont nous avons lu un article dans « Option Finance » sorti en juin 2018 et qui présente une interview effectuée avec le directeur général de l'entreprise victime où il explique le déroulement de la fraude et les mesures mises en place après cette fraude telles que la sensibilisation et la formation des collaborateurs, l'inscription à une assurance contre la fraude, etc.

Donc, nous avons estimé que le cas de cette entreprise peut être très intéressant pour notre recherche. Ensuite, nous avons contacté son directeur par courrier électronique sur son adresse professionnelle en lui expliquant notre objectif de l'étude et en lui demandant de réaliser des entretiens au sein de son entreprise, dans un premier temps avec lui et/ou avec un directeur des

SI et dans un deuxième temps, avec quelques salariés de son entreprise (quel que soit le poste). Après deux semaines de notre première demande ainsi que deux relances de mails, nous avons reçu une réponse positive. Il nous a accordé le contact de son directeur des SI pour convenir d'un rendez-vous avec lui et ensuite, avec trois salariés.

D'un autre côté, afin d'élargir notre périmètre de recherche, nous avons alors contacté une personne de la chambre de commerce et de l'industrie (CCI) de la région de Bretagne qui nous a fourni un fichier ''Palmarès des entreprises Bretonnes 2018-2019'' ainsi que quelques contacts qui peuvent être intéressés par notre étude. En plus de cela, nous avons réalisé des recherches sur internet par exemple sur le site '' Societe.com'' ou le site '' Kompass.com'', qui fournit des listes d'entreprises où nous pouvons sélectionner la recherche par région, taille, secteur d'activité, etc. Nous avons centré notre recherche d'entreprises sur les critères suivants :

- Des entreprises de 10 à 250 salariés, afin qu'elles correspondent à notre définition de la PME basée sur le décret n° 2019-539 du 29 mai 2019 décret d'application (n°2008-1354) de l'article 51 de la loi de modernisation de l'économie.
- Pour simplifier notre accès au terrain, nous nous sommes limités à la « région Bretagne » (dans un rayon d'environ 100 km) ;
- Nous avons écarté les entreprises filiales d'un grand groupe où le pouvoir de décision du dirigeant, en matière de sécurité, est limité.
- Tout secteur d'activité confondu, pour comprendre l'influence du secteur d'activité sur la culture sécurité des SI.

Le fichier fourni par la CCI Bretagne contient les 500 premières entreprises en Bretagne. Après l'application du critère de taille et de structure, il restait 40 entreprises. Ajoutant à ce nombre nos propres recherches sur internet ainsi que les quelques contacts fournis par notre directeur et co-directeur de thèse, nous nous sommes retrouvés avec une liste d'environ 70 entreprises. Ensuite, nous avons cherché des contacts rattachés à ces entreprises, les mails, les numéros de téléphone et/ou les profils dans le réseau social professionnel en ligne ''Link d'In'' des dirigeants, des DSI ou des responsables informatiques. Cette recherche nous a permis d'avoir des contacts variés liés à 50 entreprises. Afin de les contacter et les toucher par notre demande, nous avons procédé de la manière suivante :

-**Envoi de 33 mails** en se présentant : notre profil, notre objectif et notre demande. Voilà un exemple de mail envoyé :

Objet : Participation étude doctorale

Olfa ISMAIL <ismailolfa@gmail.com>

À contact x

« Bonjour,

Je suis doctorante à l'IAE (Institut d'Administration des Entreprises) de Brest dans le domaine de la gestion.

Mon travail doctoral porte sur « la sécurité des systèmes d'informations au sein des PME » et dans le cadre de ma recherche, j'ai besoin de réaliser des entretiens qui me permettront de voir où en sont les PME sur ce sujet.

Permettez-moi de vous contacter afin de savoir s'il y'a possibilité de m'accorder un entretien d'une durée maximale de 30 à 45 minutes avec vous sur ce sujet en fonction de vos disponibilités ou avec un responsable informatique ou un DSI de votre entreprise.

Toutes les informations resteront strictement anonymes et confidentielles. Au terme de cette étude vous bénéficiez de l'accès aux résultats incluant des recommandations.

Je vous remercie d'avance et je compte sur votre participation.

Bien cordialement. »

ISMAIL Olfa
Doctorante et ATER en sciences de gestion, IAE Brest
Stratégie et Systèmes d'information
Tél : +33 (0) 619.67.78.71

Ce peu de détails sur le thème de l'entretien était volontaire, dans le but de ne pas biaiser les entretiens ultérieurs. Ce mail varie légèrement selon le profil de la personne qui le reçoit.

-**Envoi de 7 messages sur le réseau ''LinkedIn''** en se présentant : notre profil, notre objectif et notre demande. Nous avons gardé le même contenu que les mails envoyés.

-**Nous avons passé 10 appels téléphoniques** : en se présentant : notre profil, notre objectif et notre demande.

Les deux dernières méthodes étaient les moins efficaces, car nous avons reçu beaucoup de réponses négatives ou des non-réponses. En gros, nous avons reçu 8 réponses positives par mail. Les réponses négatives étaient liées soit au manque de temps, soit à la sensibilité du sujet et que

les personnes contactées ne souhaitent pas échanger sur le sujet. Ces explications ont déjà été évoquées dans la littérature : Kotulic et Clark (2004), expliquent ceci par le fait que le sujet est assez « envahissant » et « importun ». D'autres considèrent la sécurité des informations comme un sujet extrêmement sensible (Straub et Welke, 1998) et recommandent une approche précautionneuse lors de la réalisation de ce type d'études (Kotulic et Clark, 2004).

Dans un premier temps, nous avons rencontré la direction de chaque entreprise (dirigeants et/ou les principaux responsables) pour savoir quelles sont les mesures sécuritaires mises en place par l'entreprise et ils nous ont ensuite permis de rencontrer les utilisateurs des systèmes d'information. Nous avons décidé de faire les entretiens sur site, dans le but d'avoir une facilité dans la visite des entreprises et de leur local informatique, ce qui a contribué à notre compréhension de chaque entreprise. Cela nous a permis aussi de regrouper les entretiens pour limiter l'influence entre les acteurs, vu la sensibilité du sujet et d'optimiser nos déplacements.

Les entretiens ont duré entre 20 et 60 minutes avec une personne de la direction (dirigeant ou responsable SI) et entre 10 et 25 minutes avec les utilisateurs des SI. Chaque entretien a été enregistré après avoir eu la permission de chaque interviewé. Ensuite, chaque entretien a été transcrit afin de pouvoir tirer une plus grande partie de la « discussion ». Les normes recommandées pour une bonne réalisation d'un entretien semi directif ont été respectées (Evrard et al. 2003). Par ailleurs, ces entretiens ont respecté : d'un côté, une attitude positive en écoutant avec intérêt et attention tous les propos du répondant et d'autre côté, une attitude empathique ayant pour objectif d'être le plus proche possible du cadre de référence de l'interviewé, surtout qu'une recherche sur un sujet sensible comme la sécurité des SI exigeait un minimum de confiance mutuelle entre l'interviewé et le chercheur.

Nous avons analysé huit cas d'entreprises : ce nombre est-il suffisant pour entrer dans une logique d'exploration ? Selon Eisenhardt (1989) : *« Bien qu'il n'y ait pas de nombre idéal de cas, un nombre de 4 à 10 cas donne de bons résultats. Avec moins de quatre cas, il est souvent difficile de générer une théorie complexe et ses fondements empiriques risquent d'être peu convaincants, sauf si le cas contient lui-même plusieurs mini-cas ».*

Eisenhardt (1991) souligne l'intérêt de multiplier les cas, notamment lorsque l'objectif de la recherche est la généralisation des résultats. Selon l'auteur, les deux critères qui peuvent dicter le nombre de cas nécessaires deviennent la saturation et la réplication. Le seuil de saturation sémantique défini par Mucchielli (1986). Où on interroge des personnes jusqu'à avoir le sentiment de ne plus rien apprendre de nouveau. Quand l'on a ce sentiment, on interroge encore

une personne de plus pour confirmer qu'on n'apprend plus rien de nouveau. C'est là, le seuil de saturation sémantique. Le principe de la saturation sémantique a été adopté afin de fixer le nombre d'entretiens à 32. Selon Romelaer (2002), la règle d'arrêt intervient quand deux entretiens successifs n'apportent plus d'idées nouvelles.

Le Tableau 24 résume les principales caractéristiques des entreprises étudiées. Nous nous sommes engagés à ne pas mentionner les noms des entreprises dans un souci de confidentialité, évident et conditionnel à notre recherche.

Entreprise	**Forme juridique**	**Taille (Salariés)**	**Chiffre d'affaires (€)**	**Secteur d'activité**	**Prestataire informatique**
A	SASU	80	35.074.500	Commerce de gros	Oui
B	SARL	35	12.795.200	Commerce de gros	Oui
C	SARL	40	500.283	Service d'aménagement paysager	Oui
D	SAS	70	20.000.000	Transformation et conservation	Oui
E	SARL	30	2.138.400	Travaux d'étanchéification	Oui
F	SARL	19	2 .029.300	Commerce de détail	Oui
G	Association	250	13.389.000	Tri et recyclage, blanchisserie, atelier paysage	Oui
H	SARL	20	1.011.500	Autre transformation et conservation de légumes	Oui
Total	8				

Tableau 25 : Caractéristiques des PME étudiées

La taille de ces entreprises se situe entre 19 et 250, pour l'entreprise G qui est un cas particulier avec une forme juridique spécifique ''Association'', qui a comme structure un conseil d'administration (géré par des bénévoles) et une direction générale avec des activités salariales où nous trouvons des salariés rémunérés en contrepartie de leurs activités. La structure de cette association et son organigramme détaillé se trouvent dans l'annexe 6, avec un tableau de gestion des clés d'accès à l'entreprise G dans l'annexe 9.

Parmi ces entreprises, il y en a une qui a 5 ans d'activité, les autres sont actives au moins depuis 21 ans et 41 ans pour la plus ancienne.

Avant d'effectuer les entretiens avec les personnes appartenant aux entreprises, nous avons tout d'abord préparé nos guides d'entretien. Nous présentons nos guides d'entretien en détail dans les éléments suivants.

5.3 Guides d'entretien

Nous avons réalisé trente-deux entretiens semi-directifs, dont dix entretiens avec la direction et vingt-deux entretiens avec les utilisateurs des SI (Salariés). Nos guides d'entretien ont été complétés au fur et à mesure de nos rencontres et certaines questions ont été précisées au fil de ces derniers.

Nous avons visité les sites des entreprises pour effectuer les entretiens avec les personnes concernées. Nous étions accueillis dans les bureaux des dirigeants et des responsables, ce qui est un gage de confiance. Quand un dirigeant a assez de confiance pour parler de la sécurité des SI de son entreprise, cela peut expliquer une part de sensibilité sur le sujet.

Les entretiens avec les salariés (utilisateurs de SI) se sont majoritairement passés dans une salle de réunion ou dans leur bureau. Nous avons été avec le répondant sans la présence d'aucune autre personne. Ce qui peut garantir une bonne qualité des données (Huberman et Miles, 1991) et aucune influence sur le répondant. Nous avons pris des engagements de confidentialité pour les salariés vis-à-vis de leur hiérarchie et vis-à-vis de l'extérieur.

Nous avons essayé d'établir une relation de confiance avec chaque interviewé, d'où toutes les personnes ont accepté l'enregistrement des entretiens, ce qui nous a permis d'assurer un maximum d'exhaustivité et de fiabilité des données qui permettent par la suite d'établir des analyses de bonne qualité. De plus, grâce à l'enregistrement, nous avons évité la prise de notes, ce qui permet à l'interviewer de conserver une certaine « sagacité et vivacité » lors de l'entretien, selon Baumard et al. (1999).

Nous avons donc élaboré des guides d'entretien spécifiques pour chaque type d'acteur. Chaque guide a été préparé à partir des informations recueillies de la revue des modèles et théories. Certains thèmes sont spécifiques à chaque type d'acteur et développés dans chaque guide d'entretien.

Rubin et Rubin, (1995), ont défini trois types de questions que comportent les entretiens semi-directifs : questions principales, questions d'investigation et question d'application :

- Les questions principales, qui correspondent à l'introduction et au guide d'entretien ;
- Les questions d'investigation, destinées à compléter et à clarifier des réponses incomplètes ou floues ;
- Les questions d'application qui suivent certaines réponses aux questions principales ou permettent d'élaborer une idée ou un concept.

Selon eux, les questions d'investigation et d'application sont posées durant l'entretien et ne sont pas préparées à l'avance. Pour notre part au fil des entretiens nous avons inclus dans notre guide certaines questions de ce type. Nous avons veillé à utiliser au maximum des questions ouvertes ou des consignes plus générales, dont la formulation n'oriente pas les réponses. Nous avons également reformulé quelques réponses des participants, dans le but de permettre à ces derniers d'approfondir leur pensée et de donner de nouveaux éléments signifiants au discours.

Nous allons présenter nos guides d'entretien et les thèmes abordés pour chaque type d'acteur. Ainsi la présentation du profil de chaque répondant.

5.3.1 La direction : guide d'entretien et profil des répondants

L'objectif de cet entretien avec un (ou plusieurs) membre(s) de la direction, généralement avec le dirigeant lui-même (6 cas /8), est de déterminer le niveau de sensibilisation du dirigeant ainsi que les actions liées à la SSI qu'il a mise en place au sein de son entreprise.

Nous nous intéressons aussi à comprendre si le dirigeant donne de l'importance aux informations qui circulent dans son entreprise ainsi qu'aux systèmes qui traitent ces informations, nous l'interrogeons sur les actions qui ont été mises mais aussi sur celles à mettre en place afin de protéger les informations, etc. Nous, nous vérifions également le rôle qu'exerce le dirigeant pour impliquer ses collaborateurs dans le respect des mesures de sécurité, que ce soit de manière informelle (sensibilisation indirecte) ou de manière formelle (formation, etc.).

Quelques questions quantitatives basiques ont été posées au début de l'entretien, car nous jugeons intéressant d'affronter ces données avec nos résultats.

Le tableau 26 présente le profil de chaque membre de la direction (fonction, ancienneté, âge, genre). Ensuite, nous allons présenter les thèmes et les questions posées lors des entretiens avec la direction.

Entreprise	Prénom	Fonction	Ancienneté	Âge	Genre
A	Thiery	Directeur des systèmes d'information (DSI)	8 ans	45	H
B	Jean-Luc	Directeur général	30 ans	52	H
C	Didier	Directeur général	11 ans	54	H
D	Sten	Directeur général	7 ans	47	H
	Gabriel	Responsable informatique	5 ans	37	H
E	Romain	Directeur général	5 ans	38	H
F	Erwan	Directeur général	4 ans	35	H
G	André	Directeur général adjoint	9 ans	54	H
	Jean-Marc	Responsable des moyens généraux (dont l'informatique)	30 ans	52	H
H	Bruno	Responsable informatique et commercial	12 ans	54	H
Total	10				

Tableau 26 : profil des membres de la direction

Les dirigeants sont tous des hommes, leurs âges varient entre 35 et 54 ans et ils ont de 4 à 30 ans d'expérience. Nous avons préparé le même guide d'entretien pour tous les dirigeants ainsi que pour les DSI et les responsables informatiques. Mais il y a une légère différence entre les questions posées directement au dirigeant pour connaitre son implication et les questions posées aux directeurs informatiques à qui nous demandons les avis à propos l'implication de leurs dirigeants, au sujet de la SSI. Voici un exemple de question directement posée au dirigeant : « Que pensez-vous du rôle que vous exercez pour impliquer vos collaborateurs dans le respect des mesures sécuritaires ? » Et pour poser cette même question aux DSI ou responsables

informatiques, la question sera posée de la manière suivante : « Que pensez-vous du rôle qu'exerce le dirigeant pour impliquer les collaborateurs dans le respect des mesures sécuritaires ? »

Nous allons montrer dans le tableau suivant (tableau 27) les thèmes du guide, quelques questions liées à chaque thème, mais aussi l'objectif de chaque question. Toutes les questions posées lors des entretiens seront présentées en détails dans l'annexe 7 (y compris un guide pour les directeurs et un pour les responsables avec une légère différence entre les deux, au niveau de la partie support de la direction pour la SSI).

Thème	Sous thème	Question	Objectif
Facteurs exogènes	Contexte réglementaire	Appliquez-vous les normes ISO relatives au management de la SSI (Comme ISO 27001) ? Si oui : Quel est l'objectif de l'utilisation de cette norme et avez-vous obtenu la certification ?	Le but de cette question est de voir si le respect de la sécurité des SI va jusqu'à l'application de la norme ISO 27001 et dans ce cas, comprendre pour quel objectif et quelles raisons.
		Avez-vous déjà entendu parler du règlement général sur la protection des données (RGPD) ? Est-ce que vous avez lancé des actions de conformité ?	Notre objectif ici est de vérifier si l'entreprise se soumet à ce règlement et ensuite, de creuser plus sur les raisons et les effets de l'application de ce règlement.
	Rôle des prestataires	Que pensez-vous du rôle de votre prestataire informatique ? (En termes de service, niveau de sécurité…)	Nous cherchons à travers cette question à comprendre la relation entre le (ou les) prestataire(s) informatique(s) en termes de confiance, d'influence, de sécurité…
		Est-ce que vous avez signé une charte qui concerne la sécurité informatique avec lui ?	Question de vérification. S'il existe une charte ou des clauses contractuelles liées à la sécurité des données entre le prestataire et l'entreprise, elles engagent la responsabilité l'un envers l'autre.
		Appliquez-vous un référentiel ou une méthode d'analyse des risques informatiques ?	Si l'entreprise applique une méthode d'analyse des risques informatiques (EBIOS, MEHARI ou ISO) dans ce cas nous pouvons comprendre qu'elle met en place une procédure

Facteurs endogènes	Existence d'une évaluation des risques		plus ou moins formelle à la gestion des risques.
		Pour les risques informatiques critiques, développez-vous des plans d'action comme PRA, PCA) ?	Pour vérifier s'il y'a des plans d'action qui ont été développés pour les risques informatiques critiques (Tiré de COBIT partie PO9 : Evaluer et gérer les risques)
	Réalisation d'actions de Formation /sensibilisation	Est-ce que vous avez mis en place une formation à la sécurité informatique pour vos collaborateurs ? Si oui : Depuis quand, budget engagé… ? Si non : est-ce que ça vous intéresse comme mesure à mettre en place ?	Cette question a pour but d'investiguer si l'entreprise a mis en place une formation liée à la sécurité pour le personnel, en quoi consiste cette formation, qu'est-ce que la direction pense de son efficacité et s'il y'a un effet sur le comportement des personnes qui ont participé à cette dernière.
		Est-ce que vous sensibilisez vos salariés à la sécurité des SI ? Si oui : de quelle manière ?	Cette question peut servir premièrement à comprendre si la direction sensibilise le personnel, ce qui explique la sensibilisation du directeur lui-même. Deuxièmement, de demander quel effet a cette sensibilisation sur le comportement des salariés.
Implication de la direction	Sensibilité du dirigeant à la sécurité	Quand vous entendez « SSI ou sécurité des SI » qu'est-ce que cela vous évoque ?	Nous voulons comprendre la vision du dirigeant : Est-ce qu'il pense directement aux risques et dangers ou plutôt tout ce qui est mesures sécuritaires et défensives ? Est ce qu'il a une vision technique ou organisationnelle ?
		Quel budget avez-vous engagé pour mettre en place des mesures sécuritaires ? Et est-ce que vous êtes prêt à augmenter ce budget ?	Par cette question, nous cherchons à comprendre s'il y'a un budget consacré à la sécurité. Si oui de quelle hauteur, ce qui peut expliquer les actions concrètes de la direction et si le dirigeant est prêt à augmenter ce budget et pour quelles raisons.
		Comment gérez-vous les identités et les autorisations des utilisateurs des SI ?	Ces deux questions paraissent techniques et notre objectif est de déterminer si le dirigeant lui-même

	Actions sécuritaires mises en place (Niveau de la SSI)		a une connaissance des mesures techniques liées à la sécurité, ce qui explique son implication et deuxièmement, recenser les actions sécuritaires mises en place par l'entreprise. Ce qui peut nous permettre ensuite d'estimer le niveau de sécurité respecté dans chaque entreprise.
		Est-ce que vous testez régulièrement la sécurité de vos SI ? (Tests d'intrusion, détection des activités anormales…)	

Tableau 27 : Guide d'entretien (Direction)

5.3.2 Les utilisateurs : guide d'entretien et profil des répondants

Notre finalité de cet entretien avec les utilisateurs des SI dans chaque entreprise étudiée, est d'estimer le niveau de la culture sécurité des utilisateurs (salariés) ainsi que leurs comportements sécuritaires et comprendre les facteurs influençant cette culture et ces comportements.

Nous cherchons à comprendre comment les utilisateurs pensent et réagissent pour contribuer à la sécurité des systèmes utilisés tous les jours et de l'information qui circule dans leurs entreprises. En cas de respect et de conscience de l'importance de la sécurité, nous cherchons les facteurs qui les motivent à cette implication et dans le cas inverse, les facteurs qui freinent une telle implication. Nous nous vérifions aussi si la direction communique auprès des salariés et le rôle joué par le directeur pour sécuriser les SI de son entreprise, d'un point de vue des salariés.

Quelques questions quantitatives basiques (âge, ancienneté, fonction dans l'entreprise) ont été posées au début de l'entretien, car nous nous jugeons intéressant d'affronter ces données avec nos résultats.

Le choix des participants a été fait par la direction en fonction de la disponibilité de leurs salariés, nous avons juste demandé que, quel que soit le poste occupé, l'essentiel est que le salarié soit un utilisateur du SI de l'entreprise.

Le tableau 28 présente le profil de chaque salarié interrogé membre (fonction, ancienneté, âge, genre), ensuite, nous allons présenter les thèmes et les questions posées lors des entretiens avec les utilisateurs des SI.

Entreprise	Prénom	Fonction	Ancienneté	Genre	Âge
A	Jennyfer	Assistante de direction-RH	2 ans	F	33
	Catherine	Comptable-Clients	12 ans	F	52
	Pierre	Comptable-Fournissuers	17 ans	H	39
B	Gaétan	Responsable service conditionnement	5 ans	H	51
	Marie-Laure	Assistante administrative	5 ans	F	41
	Maxime	Assistant qualité	6 mois	H	22
C	Fabien	Chargé d'affaire	2 ans	H	37
	Robin	Concepteur en bureau d'étude	1 an	H	33
	Jonathan	Gestionnaire d'achats	3 ans	H	42
D	Sabine	Secrétaire comptable	7 ans	F	41
E	Danielle	Assistante de direction	5 ans	F	55
	Franck	Chiffreur, métreur, dessinateur	2 ans	H	38
F	Marie	Assistante direction (polyvalente)	4,5 ans	F	24
	Maïwenn	Responsable communication	2 ans	F	28
G	Pol-Lou	Coordinateur qualité, sécurité environnement	1 an	H	23
	Brigitte	Employé d'accueil	4 ans	F	61
	Mélissa	Responsable RH-Paye	3 ans	F	39
	Marie	Assistante direction	14 ans	F	51
H	Sandrine	Assistante direction	1,5	F	33
	Bénédicte	Comptable	15 ans	F	55
	Christine	Service qualité	9 ans	F	45

	Julian	Responsable production	11 ans	H	49
TOTAL	22				

Tableau 28 : profil des utilisateurs

Parmi les 22 utilisateurs interrogés, il y a 13 femmes et 9 hommes et leurs âges varient entre 22 pour le plus jeune et 61 pour le plus âgé. Leur ancienneté dans l'entreprise va de 6 mois à 17 ans. Nous allons présenter dans le tableau suivant (tableau 29), les thèmes du guide, quelques questions liées à chaque thème et l'objectif de chaque question. Toutes les questions posées lors des entretiens avec les utilisateurs, seront présentées en détail dans l'annexe 8.

Thème	Sous thème	Question	Objectif
Culture sécurité	Propriété de sécurité	Quand vous entendez « sécurité des SI » qu'est-ce que cela vous évoque ?	Comprendre la vision de l'utilisateur en ce qui concerne la sécurité : Est-ce qu'il pense directement aux risques et dangers ou plutôt tout ce qui est mesures sécuritaires et défensives ? Est-ce qu'il a une vision technique et/ou organisationnelle.
		Selon vous, qui doit être responsable d'assurer la SSI et la confidentialité des données au sein de votre entreprise ? Si la personne ne mentionne pas sa responsabilité : Vous sentez-vous obligé à respecter les mesures sécuritaires mises en place par votre entreprise ? Pour quelles raisons ?	A travers cette question, nous visons à comprendre la manière dont l'utilisateur perçoit sa responsabilité et son rôle en matière de sécurité. Est-ce qu'il se sent concerné et responsable de la sécurité des SI de son entreprise, ou c'est une affaire qui concerne seulement la direction ? Est-ce qu'il est volontairement responsable de la sécurité de son entreprise ou c'est par obligation ?
		Pensez-vous que vous contribuez positivement à la sécurité des SI de votre entreprise ? Comment ?	Dans le cas où l'utilisateur a déjà mentionné sa responsabilité de la sécurité de son entreprise, nous voulons savoir dans quelle mesure il est responsable et quelle est sa part de contribution. Dans le cas inverse, nous cherchons les causes de la non-contribution.
	Conscience	Connaissez-vous des risques ou des menaces qui peuvent influencer votre poste de travail ou les systèmes de votre entreprise ?	Nous voulons ici vérifier si les utilisateurs sont conscients des risques et menaces, en leur demandant de citer quelques exemples et de vérifier leur degré de compréhension de ces risques.
		Avez-vous une idée de comment se protéger contre ces menaces et ces risques ?	A travers cette question, nous cherchons à vérifier si la personne sait en effet comment se protéger contre les risques, que ce soit elle qui applique les moyens de protection, ou non. Notre objectif est de déterminer le niveau de conscience des mesures de sécurité par les utilisateurs.
		Est-ce que vous avez déjà rencontré un problème de sécurité ?	Cette question peut laisser la personne s'exprimer librement sur les problèmes vécus, pour ensuite comprendre

			comment il a réagi face à ces problèmes.
		A votre avis, êtes-vous capables de faire face à des problèmes de sécurité ?	Vérifier si la personne se sent capable de réagir en cas de problème ou montre des difficultés à le faire.
		A qui vous adressez-vous en cas de problème non résolu par vous-même ?	Nous cherchons ici à comprendre la relation entre l'utilisateur et la direction et surtout, examiner le rôle du directeur.
	Conformité	Participez-vous à des formations liées à la sécurité des SI ? Si oui, comment évaluez-vous cette formation ? Est-ce que certaines de vos habitudes ont été modifiées ?	Comprendre l'effet de la formation et la sensibilisation sur les utilisateurs et leur efficacité. De plus, vérifier s'il y'a une conformité du comportement des employés avec la politique, les réglementations et les pratiques de sécurité.
		Avez-vous déjà signé une charte ou des clauses contractuelles liées à la sécurité ? Avez vu déjà lu la politique de sécurité (si elle existe) ? Quelles idées avez-vous pu en retenir ?	
Comportements liés à la sécurité		Combien de fois changez-vous vos mots de passe (fréquence) ? (Poste de travail, e-mails, code bancaire…)	Nous vérifions s'il existe des comportements sécuritaires effectifs chez les utilisateurs pour protéger les informations et ainsi, éviter les risques. Nous vérifions aussi les comportements déjà automatisés dans l'entreprise, comme par exemple la mise à jour et les sauvegardes de données.
		Vos mots de passe réfèrent ils à des éléments personnels ? (Date ou lieu de naissance, date de mariage...)	
		Faites-vous régulièrement des mises à jour et des sauvegardes de vos données ?	

Tableau 29 : Guide d'entretien (Utilisateurs)

6 Les problèmes rencontrés lors de l'étude qualitative

Parmi les problèmes que nous avons rencontrés au cours de la réalisation de notre étude exploratoire, comme les difficultés de la prise des rendez-vous avec la direction des entreprises étudiées - ce qui a induit un retard et une longue durée pour mener notre étude exploratoire. -

Nous avons aussi pris l'initiative de nous déplacer directement dans les locaux de quelques entreprises (6 PME) sans prendre rendez-vous pour tester l'efficacité de la procédure, mais malheureusement, aucune de ces entreprises ne nous a contactés par la suite. De plus, nous avons été rejetés par deux entreprises. En se présentant (profil, objet de la visite) à l'accueil d'une entreprise, un responsable nous a dit : « On n'a pas d'informatique, ni la sécurité informatique, pourquoi ne pas chercher des grandes entreprises ! Nous sommes une petite entreprise et on n'a pas de sécurité ! ». Suite à ces réactions de la part des entreprises où nous n'avons pas pris de rendez-vous ou contacté à l'avance, nous avons décidé d'arrêter cette méthode. Un autre problème rencontré lors de la période de l'épidémie « Covid-19 » qui a commencé en mars 2020 et qui a duré une longue période, d'où nous n'avons pas pu réaliser les entretiens avec deux autres entreprises (secteur informatique), qui nous avaient accordé les rendez-vous en mars et avril 2020. Donc, nous avons été obligés d'annuler ces entretiens et d'éliminer ces deux entreprises de notre échantillon.

7 Analyse des données

7.1 La méthode de l'analyse thématique de contenu

Après avoir été intégralement retranscrit à l'aide d'un logiciel de traitement de texte, le contenu des entretiens semi-directifs a été analysé en utilisant la technique d'analyse de donnée thématique (Huberman et Miles, 1991) ; technique définie par Bardin (1998) comme la méthode la plus aisée, la plus répandue et la plus utile. Fréquemment utilisée en sciences de gestion, cette technique consiste à prendre le thème comme unité de signification ou unité de découpage. On procède à un découpage du texte : **verbatim** en unité d'analyse de base : **thème**, ensuite au regroupement de ces unités en catégories homogènes, exclusives et exhaustives, puis à la comptabilisation, selon des règles préétablies, leurs fréquences d'apparition.

7.2 Un codage « a prio-steriori »

Au regard de la méthode d'analyse choisie, le codage le plus approprié à notre recherche consiste en l'élaboration de catégories à priori, à partir du guide d'entretien initial, dans lesquelles les fragments de discours vont être rangés. Cependant, la complexité de la pensée humaine nécessite généralement un certain degré d'enracinement (Allard-Poesi, 2003, Gavard-Perret et Helme-Guizon, 2008). Cela se traduit par un développement de nouvelles catégories, à partir des données recueillies du terrain, entraînant un remaniement des catégories initiales.

Cette méthode de codage « a prio-steriori » (Allard-Poesi, 2003) est celle que nous avons donc mobilisée.

7.3 Le choix de l'unité d'analyse

Notre analyse a pour objectif de mieux comprendre les facteurs qui déterminent la culture sécurité et ses relations avec les comportements liés à la sécurité. Ainsi, cet objectif est centré sur le sens et non sur le langage (Helme-Guizon et Gavard-Perret, 2004 ; Gavard-Perret et Helme-Guizon, 2008). Choisir le mot comme unité d'analyse ne correspondrait pas à l'objectif de notre recherche. Seule l'unité de sens semble correspondre. Délimitée par : *« une idée ou un ensemble d'idées isolables par rapport au reste des données qualitatives et qui présente une certaine cohésion »* (Point et Voynnet Fourboul, 2006), elle est préconisée dans le cas d'analyses thématiques centrées sur le sens (Allard-Poesi, 2003).

7.4 Le choix d'une analyse assistée par un logiciel

Nous avons choisi d'effectuer le codage à travers le logiciel **Nvivo**, celui-ci étant adapté à la fois à notre objectif de recherche de sens, avec lien entre les données classées par thème (Helme-Guizon et Gavard-Perret, 2004) et notre unité d'analyse (unité de sens). Nous avons préféré bénéficier de la valeur ajoutée par ce logiciel, qu'une analyse purement manuelle où la démarche de codage est similaire qu'avec Nvivo, néanmoins ce dernier permet d'aller plus loin dans la recherche de relations entre concepts (Bazeley, 2007 ; Descheneaux, 2007). Les résultats obtenus suite à cette analyse de données seront exposés à travers plusieurs titres correspondant chacun, à un thème d'entretien.

Synthèse de la section 1 :

Cette section a été consacrée dans un premier temps au positionnement épistémologique ainsi qu'au raisonnement de notre recherche. Dans un deuxième temps, la méthodologie de notre étude qualitative a été détaillée en présentant la méthode utilisée, la collecte de donnée, le déroulement et les guides des entretiens, ainsi que la méthode d'analyse des données. La section suivante va être consacrée à l'analyse des résultats.

Section 2 : Vers une typologie des cas étudiés : analyse des résultats

Cette section du troisième chapitre représente un essai de typologie des cas étudiés, avec une typologie des PME. Ensuite, une typologie des utilisateurs des SI dans ces PME.

1. Vers une typologie des entreprises

Cette première partie de notre analyse va dans un premier temps s'attarder sur les **facteurs exogènes,** de manière à comprendre les facteurs externes qui influencent la sécurité des SI de chaque entreprise étudiée **(1.1).** Dans un second temps, nous analyserons les **facteurs endogènes,** dans l'objectif de comprendre les facteurs internes à chaque entreprise qui influencent sa SSI **(1.2).** Et dans un troisième temps, nous évaluerons la **sensibilité de chaque direction** à la SSI **(1.3).** L'objectif de cette section est de faire une classification des entreprises, selon leur niveau de sécurité.

1.1 Analyse des facteurs exogènes

Dans cet élément d'analyse, nous allons montrer la manière dont les facteurs exogènes sont présents au sein de chaque entreprise. A savoir : le **contexte réglementaire et légal**, le **rôle des prestataires de services informatiques** et **l'appartenance à un secteur d'activité.** Tout d'abord, nous rappelons les acteurs interrogés de la direction des entreprises dans le tableau suivant :

Entreprise	Prénom	Fonction	Ancienneté	Âge
A	Thiery	DSI	8 ans	45
B	Jean-Luc	Directeur général	30 ans	52
C	Didier	Directeur général	11 ans	54
D	Sten	Directeur général	7 ans	47
	Gabriel	Responsable informatique	5 ans	37
E	Romain	Directeur général	5 ans	38
F	Erwan	Directeur général	4 ans	35
G	André	Directeur général adjoint	9 ans	54
	Jean-Marc	Responsable des moyens généraux (dont l'informatique)	30 ans	52
H	Bruno	Responsable informatique et commercial	12 ans	54

Tableau 30 : Profils de la direction de chaque PME

1.1.1 Contexte réglementaire et légal

Nous allons présenter les résultats sous forme de tableaux. Ensuite, chaque tableau sera commenté :

Sous thème Normes ISO relatives à la Sécurité	Nombre d'unités	Entreprise concernée	Personnes concernées	*Exemples de verbatim*
En cours d'application	1	A	Thiery (1)	*''Alors, je vise sans être certifié, je vise à avoir la norme ISO 27000 au niveau de l'entreprise, je pense qu'on n'est pas trop loin ! Pas trop mal ! D'avoir ça, en plus on a fait appel à un prestataire l'année dernière''* (Thiery)

Pas d'application	10	B, C, D, E, F, G, H	Jean-Luc (1), André (1), Bruno (1), Didier (1), Erwan (1), Gabriel (1), Jean-Marc (1), Romain (2), Sten (1)	*''Non, c'est lourd et puis effectivement quelqu'un qui soit dédié avec une réelle responsabilité informatique pour qu'elle s'y intéresse et qu'elle mette les choses en place, ce n'est pas notre cas parce qu'effectivement on est trop petit je pense par rapport à ça oui !''* (Didier)
				''Des normes ISO non ! On n'est pas certifiés. Pour le futur il faut voir quel est l'intérêt, quelle est la lourdeur, qu'est-ce que ça implique… Quel est le coût, dès qu'on parle normes ISO, je me dis qu'on est une petite entreprise, les moyens restent limités néanmoins rester vigilant sur tous les points qui peuvent être critiques dans le pilotage de l'entreprise l'informatique en un. Oui, je peux jeter un œil sur le sujet, je ne suis pas fermé du tout. Je reste prudent : il faut voir ce que ça implique et quel est le coût.'' (Jean-Luc)
				Non, je ne connais pas ! (Sten)

Tableau 31 : Les normes ISO relatives à la sécurité, position des entreprises

Une entreprise sur 8 qui est en cours d'application et vise la certification de la norme ISO qui concerne la sécurité des SI. Pour le reste des entreprises, soit le dirigeant ne connaît pas l'existence de cette norme, soit il pense que c'est une procédure lourde et coûteuse pour une petite entreprise.

Sous thème RGPD	Nombre d'unités	Entreprise concernée	Personnes concernées	*Exemples de verbatim*
Application	2	A, B	Thiery (1), Jean-Luc (1)	*''en règlementation RGPD, je n'ai pas trop peur, mais au moins comme ça on a un DPO mutualisé, il fallait nommer quelqu'un en interne, et embaucher quelqu'un, c'est pour ça qu'on a pris un DPO en mode mutualisé aussi devient RSSI, comme j'ai dit je peux pas juger, je peux pas être parti de l'RSSI, et mon équipe ne peux pas être RSSI, donc on a pris une personne externe, qui est du coup le RSSI et qui nous audite, tous les ans''.* (Thiery)
				''Tout à fait, on a pris contact avec une société qui accompagne les entreprises dans les SI et on a une personne d'un profil plutôt juridique qui nous accompagne. Convenu avec elle d'un accompagnement de 4 heures, 2X2h. Donc elle a déjà fait les deux premières heures pour une formation de découverte ! Qu'est-ce que l'RGPD ! Et donc on a identifié au sein des équipes une personne, ce n'est pas délégué mais un DPO, le nom officiel, c'est pour les entreprises les plus grandes mais comme même on voulait identifier une personne référente sur le sujet '' (Jean-Luc)

Demande l'avis du prestataire sur l'RGPD	3	D, F, E	Erwan (1), Sten (1), Romain (1)	*''Oui en fait, du coup on fonctionne uniquement avec des prestataires. On s'assure que les prestataires eux se sont bien mis à jour. Après, on n'est pas très (très) exposés, puisqu'on a une carte de fidélité dématérialisée sur laquelle on n'a vraiment pas beaucoup d'informations et même rien si le client ne veut rien donner, on ne demande rien, il n'est pas obligé de nous donner son nom. Ensuite après pour les salariés, tout est centralisé dans le logiciel de paye donc pareil, en fait c'est plutôt via nos prestataires qu'on s'assure que ceux-ci soient en règles''.* (Erwan)
				''Oui, oui disant qu'on s'est assurés auprès de nos prestataires qu'on était conformes, voilà, après sur la partie, on avait vérifié sur la partie personnelle et on n'avait pas de choses qui étaient non conformes avec les données clients et à l'RGPD, nos logiciels étaient conformes.'' (Sten)
En cours d'étude	3	G	André (2), Jean-Marc (1)	''*Donc, on en est au début, c'est à dire sur ce qu'on a prévu : moi je suis responsable de cette action en lien avec Mélissa, qui s'occupe donc de la gestion du personnel.''* (André)
				''On est en cours, donc, on doit faire un audit de toutes les personnes au niveau du site pour voir ce qu'il utilise et où ! C'est déjà la preuve, c'est déjà une première étape ; la preuve, quand il y a plusieurs étapes en RGPD qui donc où se trouve à appuyer un petit peu l'information déjà pour dégrossir les choses. Et après on

				mettra sans doute un plan d'action en fonction de ce qu'on doit retrouver des écarts.'' (Jean-Marc)
Pas d'application	2	C, H	Didier (1), Bruno (1)	*''Au moment on a entendu parler, mais on n'a fait aucune action de conformité. Et on traine le plus longtemps possible, à ce qu'ils nous disent quelque chose. On recueille peu de données personnelles, on est sur B to B. On a une certaine base de gens qui nous connaissent avec qui on communique. Et voilà, on n'a pas mis un responsable RGPD, on n'a pas passé une action particulière, on a un ERP qui est capable de prendre ça en compte mais pour l'instant, on s'en fiche !''* (Bruno)

Tableau 32 : Niveau de conformité à l'RGPD

En ce qui concerne l'RGPD, sur les **8** entreprises interrogées, **2** entreprises ont déjà lancé des actions de conformité à l'RGPD et ont nommé un délégué à la protection des données (DPO), qui est l'RSSI pour l'entreprise A et un DPO - qui est un salarié - pour l'entreprise B. **3** dirigeants affirment qu'ils ont demandé l'avis de leurs prestataires sur la conformité vis-à-vis l'RGPD, mais sans aller plus loin. Pour l'entreprise **G**, elle est en cours de lancement des actions pour être conforme à l'RGPD. Et enfin, **2** entreprises sur **8** n'appliquent aucune action de conformité à l'RGPD.

Accompagnement sur la sécurité

Parmi les 10 acteurs de la direction interrogés, 2 acteurs expriment leurs avis sur un accompagnement des pouvoirs publics à l'instar des Chambres de Commerce et d'Industrie

(CCI). Tel que le dirigeant de l'entreprise B qui annonce : « *Je me suis rendu en fait à la CCI, qui organisait des rendez-vous en fin de matinée de trois quarts d'heure avec des prestataires. Ce que j'ai fait et c'est suite à cette rencontre que nous avons sollicité cette entreprise de la gestion des SI qui m'a amené du coup à mettre en place la formation sur l'RGPD. Donc, c'est eux qui nous accompagnent sur l'RGPD mais on n'est pas allés plus loin sur la question de sécurité, je n'ai pas été au-delà, je pense que je vais mettre ce sujet dans mes prochains axes de travail sur la sensibilisation des équipes et de faire appel à un prestataire externe pour y prouver notre SI et notre système de sécurité* » (Jean-Luc).

Ce même dirigeant exprime un besoin d'accompagnement sur le sujet de la sécurité : « *Donc on sait que la menace est là et bien présente dans notre environnement. Comment l'appréhender ! Comment la maitriser, ça reste un sujet ! On fait mieux aujourd'hui, j'ai le sentiment qu'il y a un chemin à faire. Oui ça m'intéresse un accompagnement aux dirigeants sur le sujet, je pense que c'est un vrai sujet actuel et encore plus de demain »* (Jean-Luc). A son tour, le responsable informatique de l'entreprise D formule son avis de la manière suivante : « J*'ai été une fois à la CCI suivre une formation en une conférence sur les risques liés à l'informatique. C'est très intéressant mais derrière il n'y avait rien, je ne sais pas à qui me référer par rapport à ça. Dès qu'on parle de sécurité, on ne sait pas à qui faire confiance en fait. C'est surtout ça qui me freine aussi* » (Gabriel).

1.1.2 Appartenance à un secteur d'activité

Comme suggéré suite à la revue de la littérature, et plus précisément au niveau de notre première orientation de recherche, l'appartenance à un secteur d'activité sensible à la sécurité influence positivement la culture sécurité SI dans la PME. Nous avons relevé à partir des discours cet aspect, tel que le directeur de l'entreprise F (secteur commerce de détail) : *« Je n'ai rien à voler ! Plutôt que de dérober de l'information sur mon ordinateur, il suffit de me le demander et je vous donne accès à ma boite mail, je n'ai rien en fait ! Je n'ai rien de confidentiel, évidemment ce sont des choses qui peuvent intéresser la concurrence mais par curiosité en amitié, ils ne feront jamais rien, c'est des accords que j'ai avec des fournisseurs, savoir si j'ai 13% ou 18% de remise ça ne va pas aller faire des miracles chez eux, ensuite, en réalité, je n'ai absolument rien de sensible comme informations sur les postes de travail* » (Erwan).

Le directeur de l'entreprise E (secteur travaux d'étanchéification) qui exprime : « *Aujourd'hui, moi je vais me considérer comme étant purement anonyme, on n'est pas sur du stratégique, on a des données commerciales comme n'importe quelle entreprise, quelle que soit son activité.*

On est dans un domaine tellement banal que finalement, je ne vais pas considérer avoir un besoin de protection premium » (Romain).

Le salarié de l'entreprise B exprime son point de vue en ce qui concerne le secteur d'activité : « *Donc oui, je comprends que c'est assez important ce genre de choses-là, il y'a vraiment des données importantes à protéger dans l'entreprise et encore, on est qu'une entreprise agro-alimentaire, il y'a des secteurs où vraiment c'est plus important, je pense vraiment totalement au nucléaire et tout ça ou là pour le coût, le niveau de sécurité est très (très) impressionnant »* (Maxime).

1.1.3 Rôle des prestataires de services informatiques

Toutes les entreprises étudiées font recours à un prestataire ou une société externe, qui gère leur informatique ou une partie de l'informatique. Nous avons pu identifier les relations entre les entreprises et leurs prestataires informatiques. Certains des acteurs interrogés évoquent une relation de **confiance** avec le prestataire, tels que le responsable informatique de l'entreprise **D** et le directeur adjoint de l'entreprise **G** : « *Comme je vous le disais tout à l'heure, on n'a pas à proprement parler, d'informaticiens dans l'entreprise qui ont une culture d'informatique donc effectivement on a fait le choix de ne pas multiplier en interne les personnes ressources, puisque c'est un coût important aussi et donc on fait confiance au prestataire qui a un rôle important pour nous, parce qu'on lui délègue notre infogérance donc on essaie de faire des points réguliers avec lui* » (André). Contrairement à ces deux acteurs, le dirigeant de l'entreprise **B** qui exprime une **confiance limitée** ou une **insatisfaction** vis-à-vis de ses prestataires : « *Leurs rôles aujourd'hui d'être forces de conseils, fin j'ai quelques doutes que ce rôle soit pleinement rempli, en tout cas c'est moi qui sensibilise mes interlocuteurs et je les fais part de mes interrogations, mais aussi de mes craintes à ce sujet. Et ces craintes émanent de mes échanges avec notre assureur, qui est très vigilant sur ce sujet-là. Et donc, j'en parle avec eux régulièrement mais ! Par exemple, on devrait faire un test de récupération de données pour bien faire les choses aujourd'hui et ça n'a pas été fait ! Et je ne sens pas un engouement particulier de la part de notre prestataire pour réaliser ces tests et pourtant, ça me rassurerait de le faire et que ça fonctionne comme il le faut. Et régulièrement, quand on a notre audit mené par notre assurance, c'est un sujet qui revient. Ils sont dans l'attente de la conduite de ce test de restauration de données »* (Jean-Luc).

D'autres acteurs déclarent que leurs prestataires ont un **rôle de conseil et de support technique**, directeur et responsable informatique de l'entreprise **D**, responsable moyen

généraux et informatique entreprise **G,** directeur de l'entreprise **F,** directeur de l'entreprise **C** et directeur de l'entreprise **E** : « *Après, son rôle aujourd'hui va être plutôt quand même de support téléphonique, ça oui, il a quand même un rôle important si a nécessité mais ce n'est pas automatique. Tu n'es pas rentré dans un jeu de contrat premium où j'ai un gars qui vient me voir en permanence pour voir ce qui se passe* » (Romain).

« *Alors, son rôle est lié : plus de conseils et de moyens techniques au niveau des systèmes d'information, après on a fait des vérifications des mises à jour Windows ce genre de choses, c'est un peu ça son rôle à mon sens son rôle de conseil et de propositions de moyens techniques au niveau de structure* » (Jean-Marc).

« *Le rôle, bah, il est garant de pas mal de choses en fait, en réalité, il est garant de pas mal de choses notamment, bah lui gérer ses évolutions et fournir un service tout le temps fonctionnel parce que moi je suis ouvert 7 jours sur 7, fermé 2 jours par an uniquement, donc il faut absolument que ça fonctionne à chaque instant qu'on décide de l'utiliser ou pas mais ça se passe bien, voilà, ce sont des acteurs de premier rang tous, donc il n'y a aucune difficulté* » (Erwan).

Pour le DSI de l'entreprise **A**, le prestataire audite l'entreprise, joue un rôle de l'RSSI et du DPO : « *Donc on travaille avec le groupe « X », et son rôle est justement de faire les audits, et de jouer le rôle de la RSSI et DPO* » (Thiery). Et finalement pour l'entreprise **H**, le responsable commercial et informatique exprime une relation **non stable** avec leur prestataire puisqu'ils sont en train de chercher un nouveau prestataire, « *difficile de répondre parce qu'on est en train d'en changer. On avait un prestataire pendant des années et puis il est en train de se casser la gueule donc on est en train de regarder autour de nous quel prestataire il pourrait y avoir ! On cherche quelqu'un qui établit et qui est connu mais qui a un coût relativement modeste, on n'a pas des gros budgets sur les machines* » (Bruno). Nous avons investigué s'il existe une charte informatique ou des clauses contractuelles qui concernent la sécurité signée avec les prestataires. Le tableau suivant montre si les entreprises engagent des mesures pareilles, ou non.

Sous thème Charte et clauses contractuelles	**Nombre d'unités**	**Entreprise concernée**	**Personnes concernées**	***Exemples de verbatim***
Absence de charte et de clauses	6	B, C, D, E, F, H	Bruno (1), Erwan (1), Gabriel (1), Jean-Luc (1), Romain (1), Sten(1)	*'' Non aujourd'hui on n'a pas fait ! La réponse est succincte mais c'est la réalité* '' (Jean-Luc)
Clauses contractuelles	1	A	Thiery (1)	*''Oui, on a un contrat''* (Thiery)
Existence d'une charte mais qui n'est pas à jour	2	G	Jean-Marc (2)	*''On a eu, elle n'est pas à jour, il est à revoir, donc c'est une vieille charte, ça mériterait aujourd'hui d'actualiser''*. (Jean-Marc)

Tableau 33 : Chartes et clauses contractuelles liées à la sécurité

Donc, une entreprise sur 8 a dans le contrat des clauses qui concernent la sécurité informatique (entreprise **A**). Pour l'entreprise **G**, elle a une charte avec son prestataire, mais qui n'est pas actualisée depuis un moment. Pour le reste des entreprises **B, C, D, E, F** et **H** elles n'ont ni des chartes ni des clauses contractuelles qui stipulent la sécurité informatique avec leurs prestataires.

1.2 Analyse des facteurs endogènes

1.2.1 La gestion des risques liés aux SI

Sous thème Référentiel ou méthode	Nombre d'unités	Entreprise concernée	Personnes concernées	*Exemples de verbatim*
Existence de référentiel ou méthode de gestion de risques	4	A, B, G	Thiery (1), Jean-Luc (1), André (1), Jean-Marc (1)	*''Oui, on essaie d'analyser, en fait, on a cette culture-là de l'entreprise du document unique d'analyse des risques. Le risque informatique, c'est un risque parmi d'autres quand on intègre aussi notamment''* (André)

				Alors, moi j'ai le référentiel ISO 27000, que j'ai en tête et que j'utilise depuis maintenant de nombreuses années, 2006 la première année où j'ai mis en place, pas ici mais ailleurs, donc je connais ce modèle, que j'essaie d'appliquer…Mais voilà un modèle de norme que j'essaie de mettre en place. (Thiery)
Pas de référentiel ou méthode de gestion de risques	6	C, D, E, F, H	Bruno (1), Didier (1), Erwan (1), Gabriel (1), Romain (1), Sten (1)	*''Non pas du tout, je ne sais pas comment les autres pratiquent ?! Peut-être parce ce qu'on n'a jamais eu le problème. Le jour où on aura un problème, on se dira qu'il fallait faire quelque chose ! C'est vrai qu'on a confiance entre nous mais !''* (Didier)
				''Non pas du tout du tout on en a parlé souvent mais on n'a pas eu de contact, je ne sais pas à qui m'adresser'' (Gabriel)

Tableau 34 : Référentiels ou méthodes liées à la gestion des risques

Trois entreprises (A, B, G) appliquent ou se réfèrent à un référentiel ou une méthode de gestion de risques, tels qu'ISO 27000, contre cinq entreprises (C, D, E, F, H) qui n'appliquent aucune méthode de gestion de risques informatiques.

Sous thème Evaluation des risques identifiés	Nombre d'unités	Entreprise concernée	Personnes concernées	*Exemples de verbatim*
Evaluation partiel et non structuré	1	H	Bruno (1)	*On n'a rien de structuré dans la démarche ! Juste on a un petit peu d'expérience, on se renseigne, on prend des avis à droite et à gauche et puis en fonction de ça, on essaye d'analyser les risques et de faire au mieux en fonction de nos moyens, quoi !* (Bruno)
Existence d'une évaluation de risques	3	A, G	André (1), Thiery (1)	*''Alors j'applique des matrices de risques, quand il y'a besoin de les appliquer, sinon pour du courant non, il n'y a pas trop d'utilité à appliquer la matrice des risques dans tous les projets. Dans les projets qui sont contraignants, oui, il faut le faire pour être sûr de ne rien oublier''* (Thiery)
Pas d'évaluation de risques	6	B, C, D, E, F	Didier (1), Erwan (1), Gabriel (1), Romain (1), Sten (1), Jean-Luc (1),	*'' Non on n'a jamais mis de test, on ne s'est pas mis dans une situation de risque pour évaluer notre niveau de résistance à une attaque. Non, pas aujourd'hui''* (Jean-Luc) *''Non ! Disant par l'intermédiaire de ce prestataire-là, la partie matérielle s'il y'a des évolutions on est tenus au courant des évolutions mais en revanche, de manière générale on ne fait pas''* (Sten)

Tableau 35 : Evaluation des risques informatiques identifiés

Deux entreprises (A, G) sur huit évaluent le niveau des risques identifiés, une entreprise (H) qui évalue partiellement le niveau de risque informatique et de manière non structurée '' *On n'a rien de structuré dans la démarche ! Juste on a un petit peu d'expérience, on se renseigne,*

on prend des avis à droite et à gauche'' (Bruno). Enfin, cinq d'entre eux (B, C, D, E, F) qui ne font pas une évaluation des risques liés à l'informatique.

Sous thème Plans d'actions	Nombre d'unités	Entreprise concernée	Personnes concernées	*Exemples de verbatim*
Existence de plans d'actions pour les risques critiques	9	A, D, E, F, G, H	Thiery (1), Romain (2), André (2), Jean-Marc (1), Erwan (1), Bruno (1), Gabriel (1)	*''On a un bilan aussi, il y a une journée aussi PRA de simulation de reprise, un plan de reprise d'activité qui est fait tous les ans et une journée de PRA avec un débriefing''* (André)
				''Donc on a mis en place un PRA, PCA, avec RTPO à 15 minutes, de fait de la réplication, on est en train de regarder pour viser le 0. Il y'a des solutions maintenant qu'on a fait le choix de prendre ce PRA, PCA créés en 2017, maintenant, il existe des solutions techniques qui permettent d'avoir un RTPO à 0, je suis en train de regarder, c'est le curseur entre coût et technologie'' (Thiery)
Pas de plans d'actions	2	B, C	Didier (1), Jean-Luc (1)	*''Pour le PCA, c'est un dossier, il y'a un coût, il faut consacrer du temps ! Aujourd'hui, l'entreprise n'a pas les moyens de mener ça, aujourd'hui ce n'est pas dans les projets immédiatement, peut être un jour mais aujourd'hui on a d'autres dossiers qui sont plus prioritaires que celui-là''* (Jean-Luc)

Tableau 36 : Plans d'actions pour gérer les incidences de sécurité

Les entreprises (A, D, E, F, G, H) mettent en place des plans d'actions pour les risques informatiques critiques tels que les PCA, PRA et des sauvegardes (historique des années

précédentes pour reprise des données). Deux entreprises (B, C) ne mettent pas en place des plans d'actions pour les risques critiques.

1.2.2 Actions de formation et sensibilisation

Sous-thème Formations et sensibilisations	Nombre d'unités	Entreprise concernée	Personnes concernées	*Exemples de verbatim*
Actions de formation et sensibilisation pour les utilisateurs	3	A	Thiery (3)	*''Alors, on a mis en place une formation de sensibilisation à la SSI, tous les ans, tous les ans on a 15 personnes qui vont en formation, ça fait 10%, tous les ans 10% des utilisateurs qui partent en formation''* (Thiery)
Existence d'une sensibilisation	4	D, G	André (1), Gabriel (1), Sten (2)	*''En fait, je les sensibilise quand moi-même j'ai des événements dont j'entends parler qui me resensibilisent et je les partage en fait''* (Sten) ''*On essaie de sensibiliser les gens. On vient de mettre en place par exemple VADESECURE sur les boîtes mail, un système un logiciel qui analyse les mails entrants. Donc on a sensibilisé les gens, on est allés, c'est Orange qui faisait une réunion''* (André).
Pas de sensibilisation ni formation	4	E, F, H, C, B	Bruno (1), Didier (2), Jean-Luc (1), Erwan (1), Romain (1)	*''Non, non, mais c'est vrai, il y a des entreprises qui interdisent certains sites Internet au travail Facebook par exemple. C'est vrai qu'on a pleins de choses qu'on ne vérifie pas, ce sont des données qui partent comme ça !'' (Didier)*

Tableau 37 : Actions de formations et sensibilisation à la SSI pour les utilisateurs

Seulement une entreprise (A) sur 8 met en place une formation à la SSI et sensibilise les utilisateurs des SI. Deux entreprises (D, G) sensibilisent les utilisateurs et cinq entreprises (E, F, H, C, B) ne font ni de formations, ni de sensibilisation à la SSI pour ces derniers. Pour l'entreprise A qui met en place une formation à la SSI, le tableau suivant montre le contenu de cette formation et son efficacité selon le DSI de cette entreprise.

Formation entreprise A	***Exemples de verbatim***
Contenue	*''Le contenu de la formation, c'est une formation de sensibilisation sur les risques informatiques, non seulement les risques professionnels, mais aussi les risques personnels, parce que la sphère professionnelle et la sphère personnelle au niveau des utilisateurs ça s'amalgame, donc il faut qu'on prenne en compte aussi leurs usages personnels dans cette formation-là, ça leur permet aussi de découvrir des choses et de stopper des choses aussi, qu'ils feraient ou qu'ils font au niveau personnel''* (Thiery)
Efficacité	*"A ce jour on a 45 personnes qu'ont été formées, ça représente la moitié des utilisateurs des SI, certains se sont demandés pourquoi ! Très clairement d'autres étaient très intéressés, c'est assez mitigé, on a sensibilisé les gens ceux qui étaient en formation maintenant, sont les premiers à revenir vers nous pour savoir est ce que tu penses que ce mail est un faux ?! Est-ce que tu crois là il y'aura un souci ?!… Oui, on a des retours là-dessus, je pense que les gens ont compris le pourquoi de cette formation, même si on a qui râlent !''* (Thiery)

Tableau 38 : Contenu de la formation et son efficacité vue par la direction de l'entreprise A

Avis de la direction sur l'implication et la sensibilité des utilisateurs à la SSI

Lorsque les acteurs de la direction sont interrogés sur la sensibilité des salariés sur le sujet de la SSI, nous constatons que parmi eux, certains pensent que les utilisateurs sont sensibles et impliqués dans la SSI en **fonction de leur poste** : « *Oui je pense que les 50 personnes concernées par l'informatique sont quand même des gens responsables donc. Disons qu'on n'a pour l'instant pas eu de soucis de blocage. Ceci étant, je pense que les gens sont par nature ou*

par leur fonction, assez sensible. Quelqu'un qui travaille à la RH ou travaille à la comptabilité à la gestion par la nature de son travail est sensibilisé sur le risque informatique » (André).
« *C'est parce que pour la plupart de ceux qui s'évoluent sur les postes, ils ont conscience que c'est leur outil principal. Donc si demain ils n'ont plus cet outil, ils ne peuvent plus travailler. Donc voilà en général le besoin, on aime ce qu'on fait donc on fait en sorte que ça dure. Donc on prend soin du matériel et on essaie de faire moins et de se mettre en danger le moins possible. Nous l'entreprise après, c'est vrai que les gens s'impliquent vraiment et font attention dès qu'ils sont sur Internet, font attention à tout ce qu'ils font et qui communiquent. Et s'il y a le moindre doute, le circuit de communication s'ouvre* » (Gabriel).

D'autres pensent que c'est lié au **caractère de chacun** : « *On va dire oui ! C'est une bonne question ! C'est le caractère de chacun, chacun leur point de vue, aujourd'hui on fonctionne vraiment sur la confiance* » (Bruno).

Et un dirigeant pense que la SSI **n'intéresse pas les utilisateurs** de son entreprise et qu'ils cherchent que ça soit fonctionnel facilement : « *Globalement, ça ne les intéresse pas. Ce qu'ils veulent, c'est juste que ça fonctionne et que ce soit simple. Voilà comment, ils ne sont absolument pas sensibilisés, ni très sensibles au sujet tout ce qu'ils veulent c'est : plus c'est simple mieux c'est ! Donc voilà, après on essaie malgré tout sur les grands principes de base mais, globalement non ce n'est pas du tout quelque chose ! Qui ne sont pas concernés quoi c'est tout !* » (Erwan).

D'autres pensent que les salariés **n'ont pas le choix et qu'ils doivent respecter** les mesures sécuritaires : « *Ils n'ont pas le choix ! Tout ce qui est sécurité obligatoire, anti-virus c'est mis à jour, installé sur la machine qui ont ça, ils n'ont pas le choix. La connexion sur les machines, ils ne peuvent pas faire autrement que mettre leur profil utilisateur et un mot de passe donc là, ils n'ont pas le choix !* » (Thiery).

« *En orientant comme ça, ils n'ont pas trop le choix je pense !* » (Jean-Marc).

Enfin, deux dirigeants pensent que les utilisateurs **respectent au mieux les quelques mesures en place** : « *Ils ont une mission plutôt, je dis ça comme ça, ils ont une mission à remplir. Donc il n'y a aucune restriction par rapport à ça, après ils vont appliquer des règles de bon sens que chacun appliquerait - je pense - chez lui* » (Romain).

« *Ils les respectent au mieux par rapport à ce qu'on leur a demandé vu qu'on n'a pas demandé grand-chose »* (Sten).

1. 3 Sensibilité du dirigeant à la sécurité

1.3.1 La sécurité vue par les acteurs de la direction

Tout d'abord, nous allons examiner dans le tableau 39 les verbatim représentant la sécurité vue par les dirigeants. Cela permet de se faire une première idée de leur implication. Nous avons constaté que certains expriment tout ce qui représentent les risques et menaces dans leurs définitions de la sécurité, d'autres plutôt tout ce qui est sécurité et protections et le reste, les deux aspects au même temps sécurité et risques.

Sous thème Définition de la sécurité	**Entreprise concernée**	***Exemples de verbatim***
Aspect sécuritaire	A	*''Nous aurons tout le loisir de discuter SSI, PRA, PCA, ISO 27000, ISO 20000''* (Thiery)
	G	*''ça m'évoque la sécurité des données entrantes ou sortantes de l'Association, de préserver l'intégrité des données, d'éviter qu'il y ait des personnes qui pénètrent dans notre système, pour détourner ou capter de l'information essentiellement''* (André)
	D	*''Il y a l'aspect matériel l'aspect sécurité des réseaux. Et puis, il y la confidentialité des données, des données orales je dirais et du papier bien sûr mais c'est surtout l'aspect « personne », l'aspect humain et l'aspect matériel technique et matériel de domaine que ça m'évoque''* (Sten)
Aspect risques	B	*''Bah, la notion de risque qui est à mon sens un sujet important. Qui a été identifié d'ailleurs, par notre assurance. On a été amenés à travailler avec le groupe ''X'' sur un audit global de la performance de l'entreprise et on a ressorti effectivement que le profil de l'entreprise, on a un niveau de risque qui n'était pas à négliger ce n'était pas un risque élevé mais un risque à prendre en compte.''* (Jean-Luc)
	C	*''Le piratage de documents éventuellement ça nous est arrivé une fois deux fois ! Deux fois effectivement par le biais de mails. On a perdu une bonne partie des données, la première fois. On a perdu 15 jours de travail je crois. Et l'année dernière on a perdu 10 jours aussi. Le prestataire était en congés en plus, bref c'était le bordel. On a essayé*

		de rattraper nos trucs mais on a perdu une dizaine de jours, on a restauré ce que nous pouvons déjà''(Didier)
	E	*''Principalement notre outil informatique. Sur la communication extérieure de nos éléments. Les éventuels piratages qu'on peut avoir en interne, la fuite des données accessoirement. C'est principalement ça que ça m'évoque''* (Romain)
Aspect sécurité et risques	H	*''Cela évoque deux choses pour moi, c'est déjà sécurité dans le temps paraît tout crash, destruction, vol ou incendie, en ayant des sauvegardes à jour et plus facilement récupérables. C'est le premier truc. Le deuxième truc de sécurité, c'est par rapport à des menaces extérieures, donc avoir des antivirus à jour, des pares feu, etc.''* (Bruno)
	F	*''Beaucoup de choses naturellement dont pleines composantes d'abord la sécurité en va dire de l'information en fait, en réalité plutôt que ce soit celle des magasins : comptable, fiscal, logistique, stocks et tout ça ! Ou alors, celle de mes clients avec tout ce système de carte de fidélité.* *Donc voilà ce que ça m'évoque, quelque chose de vulnérable. Et aujourd'hui pour nous le plus important, c'est tout ce qui gère l'opérationnel, mes systèmes d'encaissement, mes TPE, ma vision entre les deux magasins mes sauvegardes''* (Erwan)
	G	*''Deux choses, il y a cette sécurité au niveau des facteurs externes et aussi de l'interne. Donc, ces signaux externes sont plus sensibilisés effectivement, ces mises à jour Windows, fin tout ce genre de choses, des renouvellements de parc. Après, c'est au niveau donc on a aussi effectivement des intrusions externes et internes. Donc ça prend en compte la formation au niveau des salariés et aussi, ça prend en compte la partie matérielle au niveau de sécurités au niveau informatique firewall et des systèmes de sécurité via les mails ou ce genre de choses pour avoir un maximum de sécurité de notre système d'information''* (Jean-Marc)

Tableau 39 : La sécurité vue par la direction des entreprises

Lorsque nous avons demandé à chaque dirigeant/responsable, qu'est-ce que ça lui évoque la notion de sécurité des SI, nous avons remarqué qu'il y'a des dirigeants qui évoquent l'aspect sécurité seulement (A, G (directeur adjoint), D), il y en a d'autres qui parlent seulement de l'aspect risques (B, C, E) et enfin quelques-uns d'entre eux évoquent les deux aspects sécurité et risques (H, F, G (responsable informatique)).

1.3.2 Intérêt pour la sécurité SI, exprimé par la direction

Sous thème Intérêt pour la sécurité	**Entreprise concernée**	***Exemples de verbatim***
Faiblement intéressé	F	*''En fait c'est un sujet auquel je m'intéresse quand j'ai un problème. Lors de la mise en place du système informatique qui date d'il y a cinq ans. On est sur une version qui date de cinq ans, on réfléchit une bonne fois pour toutes dans les grandes lignes au principe de sécurité. Ensuite, on les met en place et six mois après, ils sont obsolètes. Donc on met les grands principes en place, quelques semaines après ils sont déjà obsolètes mais on passe à autre chose, on n'a pas le temps. Et du coup c'est quelque chose que je vérifie, juste que mes sauvegardes se passent bien une fois par semaine. Mais ça s'arrête là. Rien de plus ! ''* (Erwan)
Moyennement intéressé	D	''Oui, oui ça m'intéresse. Je n'ai pas forcément d'exemple mais disons qu'on a certaines choses qui permettent une protection je pense correcte mais pas parfaite, pas parfaite du tout.'' (Sten)
	H	''Oui bien sûr oui, oui, c'est quelque chose d'important oui !'' (Bruno)
	C	*''Ben oui bien sûr. Ouais ouais ouais. Et puis après, il y a ça. Et puis, il y a l'aspect aussi qu'on a évoqué avec le monsieur qui l'accompagne pour Google Drive, c'est que si on a un collaborateur qui s'en va de l'entreprise aussi on puisse se couper les robinets entre guillemets qu'il n'ait plus accès aux données de l'entreprise le jour où il part quoi, et ça avec Google Drive apparemment c'est assez facile''* (Didier)

	E	*'' C'est un sujet qui m'intéresse. Parce qu'on est complètement dépendants du sujet d'une certaine façon. Toute la compta, la partie commerciale etc., se fait qu'avec nos systèmes informatiques. Donc, les infos essentielles de l'entreprise sont disponibles dans l'informatique donc nécessairement oui, c'est une préoccupation. En ce qui concerne la fuite des données, donc, mes collaborateurs ont accès à des informations qui font partie de la vie et de l'entreprise. Après il n'y a pas de verrou particulier par rapport à ça, quoi !''* (Romain)
Très intéressé	G	*''Oui, il faut s'y intéresser parce que c'est un sujet important, effectivement. C'est important parce qu'on a des enjeux, on a des informations personnelles du fait du handicap des personnes on a des informations qui sont sensibles donc à préserver cette information-là. Et puis, on a aussi plusieurs sites géographiques différents, donc on essaie que dans chaque site de cette sensibilité informatique un peu commune''* (André)
	B	*''Oui clairement, oui ! Oui dans la mesure d'un risque, moi en tant que dirigeant je dois être garant de la performance de la structure et ça passe par le bon fonctionnement de l'ensemble des outils de l'entreprise et l'informatique est aujourd'hui un outil au cœur de notre quotidien donc il faut absolument que ça fonctionne. Donc effectivement, la maitrise des risques d'un dysfonctionnement, d'une attaque d'un hackeur est un paramètre à prendre en compte. Oui le sujet m'intéresse clairement.''* (Jean-Luc) *''Voilà en conclusion ce que je pourrais dire. En tant que dirigeant, c'est un sujet très technique très délicat ! On n'a pas les compétences, moi je connais l'informatique mais le réseau n'est pas du tout mon métier et donc comment faire pour maitriser ce risque qui l'on sait, est de plus en plus présent''* (Jean-Luc)
	A	*''La direction est partie prenante dans cette mise en place de cette formation''* (Thiery) *''Qu'on compte mettre en place dans le futur, non, je pense qu'on pourrait mettre le curseur bien plus haut, c'est-à-dire mettre beaucoup plus de contrôle, de*

		surveillance, avec un coût supérieur, en mettant par exemple les « bacs à sable », un bac à sable, ce n'est plus ni moins, un « Sand box » c'est quand vous recevez un email, cet email là avec pièce jointe, cette pièce jointe est ouverte dans un environnement virtuel qui va l'ouvrir et vérifier qu'elle ne contient pas un virus. S'il n'y a pas virus, elle arrive sur votre mail, sinon, elle sera bloquée.'' (Thiery)

Tableau 40 : Intérêt exprimé pour la sécurité des SI

Le dirigeant de l'entreprise F exprime un faible intérêt à la sécurité SI pour son entreprise. Les responsables des entreprises D, H, C, E sont moyennement intéressés et les responsables des entreprises A, B et G expriment un fort intérêt à la sécurité SI.

1.3.3 Responsabilité de la sécurité

Sous thème Responsabilité de la sécurité	**Entreprise concernée**	***Exemples de verbatim***
Dirigeant	B, C, E, F, H	‘*’C'est moi ! Sur ce plan-là c'est moi, aujourd'hui c'est moi.*’’ (Romain)
		''Et bah c'est moi !'' (Erwan)
		''C'est plutôt moi qui suis à la manette les questions en lien avec l'informatique.'' (Jean-Luc)
Direction et responsable informatique	A, D, G	*''Donc, il y a principalement le directeur général, moi-même sur le sujet et Jean-Marc''* (André)
		''Ce sera moi et le référent informatique'' (Sten)
		"En termes de décision, je valide ! En termes de décision budgétaire s'il y'a un budget à louer à ça, c'est en discussion avec les actionnaires. Les actionnaires, ça veut dire la direction du groupe'' (Thiery)

Tableau 41 : La personne responsable de la sécurité SI dans l'entreprise

Pour l'entreprises B, C, E, F, H c'est le dirigeant qui a la responsabilité et la décision en tout ce qui concerne la SSI, et pour l'entreprise A, c'est le DSI qui valide les décisions qui concernent la SSI avec la direction générale, et enfin pour les entreprises D et G, c'est le dirigeant et le responsable informatique qui peuvent prendre des décisions sur le sujet.

1.3.4 Rôle exercé par le dirigeant pour impliquer les utilisateurs (Point de vue de la direction)

Sous thème Rôle exercé	**Entreprise concernée**	***Exemples de verbatim***
Faible	C, F, H	*''On n'a pas vraiment d'actions ! Après les collaborateurs, tout le monde sait qu'il faut faire attention, à une pièce jointe dans un e-mail !''* (Bruno)
Moyen	E	*''Mais ça s'arrête à des petites infos, histoire des mails ou des choses comme ça ne va pas plus loin quoi et je n'en fais pas du ''bashing'' quotidien.''* (Romain)
Fort	A, B, D, G	*''Mon rôle est absolument essentiel, c'est moi qui donne les objectifs et de par mon empreinte va créer la culture entreprise, t'as l'esprit du bout du collectif. Donc un rôle absolument essentiel''* (Jean-Luc)

Tableau 42 : Rôle exercé par la direction pour impliquer les utilisateurs

1.4 Mesures de sécurité prises

Entreprise	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**
Test de la sécurité	x							
Mesures de prévention	x	x	x	x	x		x	x
Techniques de sécurité	x	x	x	x	x	x	x	x
Gestion des identités	x	x	x		x	x	x	x
Total mesures de sécurité prises	4	3	3	2	3	2	3	3

Matrice 1 : Niveau de mesures déjà prises dans chaque entreprise

Pour le test de la sécurité, c'est tout ce qui est tests réguliers d'intrusions ainsi que détections des activités inhabituelles et anormales du SI. Pour les mesures de préventions, il y'a les anti-virus, correctifs de sécurité, etc. Au niveau des techniques de sécurité, nous avons tout ce qui

pares-feux, compartimentage réseaux, dispositifs de sécurité entre réseaux, etc. Et enfin pour la gestion des identités, c'est l'accès des utilisateurs au SI, que ce soit de manière standardisée, avec des badges ou codes d'accès et mots de passe. L'entreprise A obtient une note de 4/4, puisqu'elle met en place les 4 mesures de sécurité. Les entreprises B, C, E, G, H obtiennent une note de 3/4, puisque 3 mesures sur 4 sont en place et finalement, les entreprises D et F obtiennent elles, une note de 2/4 pour les 2 mesures en places.

1.5 Budget consacré à la SSI

Entreprise	A	B	H
Budget sécurité (en euros)	10.000	Entre 1000 et 2000	

Tableau 43 : Budget consacré à la sécurité SI en euros par an

Pour l'entreprise A, le DSI déclare un budget destiné à la sécurité de 10.000 euros, ce qui est un budget intéressant pour une entreprise de taille moyenne. Les entreprises B et H ont un budget entre 1000 et 2000 euros pour la sécurité, pour ce qui est mises à jour et sauvegardes. Pour le reste des entreprises, les responsables ne précisent pas le budget de sécurité mais le budget total de l'informatique dont une partie pour la sécurité (mises à jour, sauvegardes etc.), est indiqué dans le tableau suivant, pour chaque entreprise (prestataires et contrat de maintenance).

Entreprise	C	D	E	F	G
Budget informatique (en euros)	5000	10.000	Entre 5000 et 6000	Entre 3000 et 5000	Environ 50.000 (Y compris la sécurité)

Tableau 44 : Budget consacré à l'informatique en euros par an

Augmentation du budget consacré à la sécurité

Quand nous avons demandé aux dirigeants s'ils étaient prêts à augmenter le budget destiné à la sécurité des SI, nous avons alors remarqué qu'il y avait des dirigeants qui étaient **prêts à augmenter** le budget de la sécurité. C'était le cas pour les entreprises **B** et **D** :

« *Et de la même façon en fait sur le SI je me dis si je mets mille, deux mille, trois mille de plus par an pour renforcer et être vraiment sûr de la maitrise de notre sécurité des SI, je le ferai mais c'est plutôt sur la question d'accompagnement en fait ! Aujourd'hui, je trouve que ce n'est pas au niveau de maturité, le niveau d'accompagnement à mon avis est perfectible* » (Jean-Luc)

« Ah oui Sten est tout à fait ouvert à ça. Il n'y aura pas de soucis si on trouve des solutions efficaces qui ont fait leurs preuves et surtout, qui peuvent nous protéger et protéger nos clients ou toute personne amenée à transiter par notre système informatique, oui, on ira vers ça » (Gabriel)

« *Oui je pense. Actuellement, je pense que notre problème n'est pas un problème matériel mais plus un problème de comportement* » (Sten)

D'autres dirigeants qui sont prêts à augmenter le budget de la sécurité mais **seulement en cas de** nécessité, et c'est le cas pour les entreprises A**, C, E** et **G :**

« Donc, on n'hésiterait pas s'il y avait besoin de mettre plus d'argent, à condition que ça couvre un risque que cet investissement va nous permettre de couvrir un risque » (André)

« *Après, il faudrait qu'il y ait une vraie valeur ajoutée à le faire !* » (Romain)

« *En cas de nécessité, si on leur prouve que pour faire quelque chose, oui !* » (Thiery)

Pour les entreprises **F** et **H,** les interrogés expriment le fait que la direction n'est pas prête à augmenter le budget consacré à la sécurité :

« On essaie de ne pas augmenter le budget, oui ! Après s'il y'a un risque avéré on le fera mais on reste ! On n'est pas convaincus, quoi ! Aujourd'hui on a l'impression qu'on a des mesures et un budget qui sont adaptés à notre activité et aux risques qu'on concourt » (Bruno)

« *Mais si je doublais mon budget admettons, aujourd'hui je n'ai aucun intérêt puisque même en cas de soucis, ça ne me coûterait pas 15 000 euros quoi ! Donc si je rajoute 3000 ou 4000 euros par an supplémentaires pour la sécurité de toute façon au bout de 3 ou 4 ans globalement ça aura coûté plus cher au préventif qu'au correctif donc, je n'ai pas un grand intérêt ! Le jour où ça arrivera où il y aura quelque chose effectivement, il y aura quelque chose de plus conséquent à effectuer, mais ça ne sera jamais complètement démesuré »* (Erwan).

Estimation de la sensibilité de la direction de chaque entreprise

Entreprise	A	B	C	D	E	F	G	H
Intérêt pour la sécurité	3	3	2	2	2	1	3	2
Rôle exercé pour impliquer les utilisateurs	3	3	1	3	2	1	3	1
Total mesures de sécurité prises*	4	3	3	2	3	2	3	3
Budget sécurité	3	1	1	1	1	1	2	1
Augmentation budget	2	3	2	3	2	1	2	1
Sensibilité estimée**	15	13	9	11	10	6	13	8

Matrice 2 : Estimation de la sensibilité du dirigeant de chaque entreprise

Grille de notation :

Intérêt pour la sécurité / rôle exercé / Budget sécurité
1 : Faible ; 2 : Moyen ; 3 : Fort

Mesures de sécurités prises
Total = 4 actions (Déjà calculé dans la matrice 1)

Augmentation budget
1 : Faiblement prêt à augmenter
2 : Prêt à augmenter en cas de nécessité
2 : Prêt à augmenter

Estimation du niveau de la sécurité des SI dans chaque entreprise

Entreprise	A	B	C	D	E	F	G	H
Norme ISO relative à la sécurité	1	0	0	0	0	0	0	0
Actions liées à l'RGPD	3	3	0	2	2	2	1	0
Chartes et clauses contractuelles	2	0	0	0	0	0	1	0
Analyse des risques (Référentiel/méthode)	1	1	0	0	0	0	1	0
Evaluation des risques	2	0	0	0	0	0	2	1
Plans d'actions (PCA, PRA)	1	0	0	1	1	1	1	1
Formation	1	0	0	0	0	0	0	0
Sensibilisation	1	0	0	1	0	0	1	0
Sensibilité estimée**	15	13	9	11	10	6	13	8
Niveau de sécurité estimé	27	17	9	15	13	9	20	10

Matrice 3 : Estimation du niveau de sécurité de chaque entreprise

Grille de notation :

Norme ISO relative à la sécurité
0 : Pas d'application
1 : Application

Actions liées à l'RGPD
0 : Pas d'application,
1 : En cours d'étude,
2 : Application partielle selon prestataire
3 : Application

Chartes et clauses contractuelles
0 : Absente
1 : Existe, mais pas à jour
3 : Existe

Analyse des risques, Plans d'actions (PCA, PRA), Formation et sensibilisation
0 : Absente
1 : Existe

Evaluation des risques
0 : Absente
1 : Partielle
1 : Existe

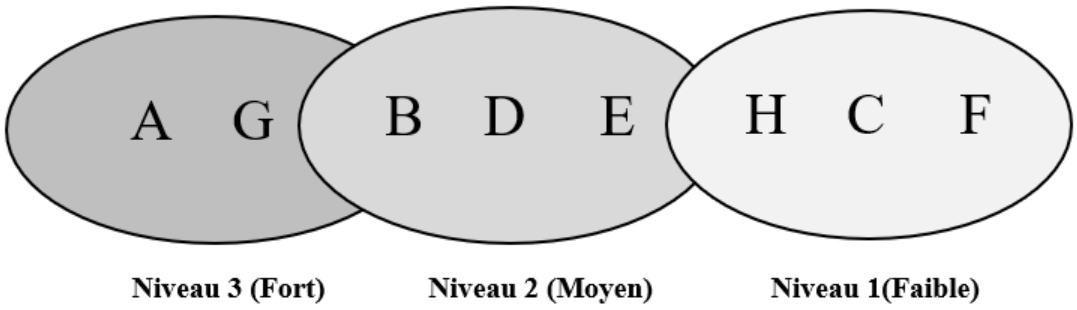


Figure 33 : Classification des entreprises selon leurs niveaux de SSI

Suite à l'analyse de chaque cas d'entreprise, nous avons pu classifier les entreprises selon leurs niveaux de sécurité des SI :

Niveau 1 : Faible niveau de sécurité

Niveau 2 : Moyen niveau de sécurité

Niveau 3 : Bon niveau de sécurité

Ces 3 niveaux de sécurité sont fixés selon des mesures **réglementaires et légales** (normes ISO, RGPD, chartes et clauses), des **mesures organisationnelles** (gestion des risques, formation et sensibilisation), **sensibilité de la direction** à la SSI (intérêt, rôle, mesures de sécurité déjà prises, budget sécurité). Nous avons donc attribué une note pour chaque entreprise sur chacune des mesures liées à la sécurité, pour enfin avoir une note globale du niveau de sécurité. Selon cette note finale, nous avons classé les entreprises dans 3 niveaux de sécurité d'où :

Niveau 1 : Entreprises **H, C, F** avec de très faibles mesures de sécurité mises en place par ces entreprises ainsi qu'une faible sensibilité de la direction à la sécurité.

Niveau 2 : Entreprises **B, D, E** avec quelques mesures de sécurité mises en place et une sensibilité moyenne de la direction (excepté la direction de l'entreprise B avec une sensibilité du dirigeant plus forte :13 points).

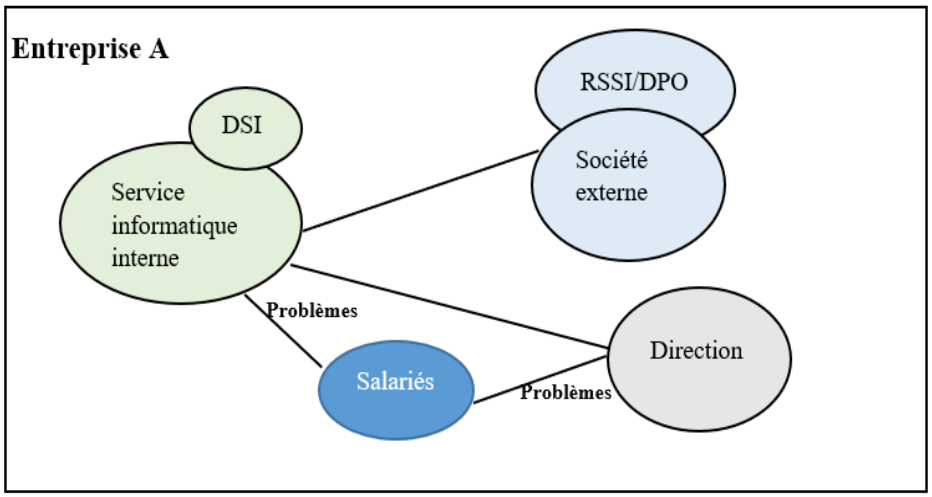
Niveau 3 : Entreprises **A et G** avec des mesures de sécurité en place et une forte sensibilité de la direction à la sécurité.

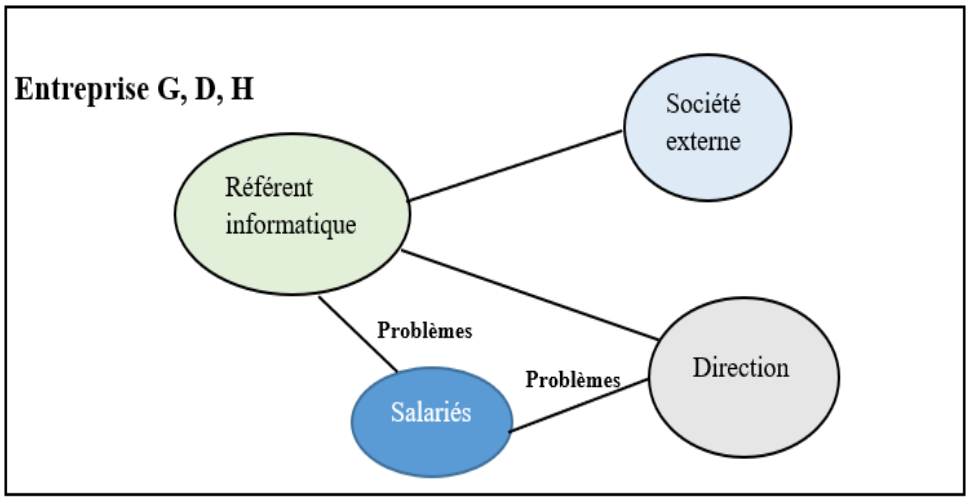
Pour l'entreprise **A** avec le plus haut niveau de sécurité, la gestion de sa sécurité SI est assurée par le service informatique interne avec un support d'une société externe qui joue le rôle de l'RSSI et du DPO. Les salariés de cette entreprise remontent les problèmes liés au SI à la direction et/ou au service informatique.

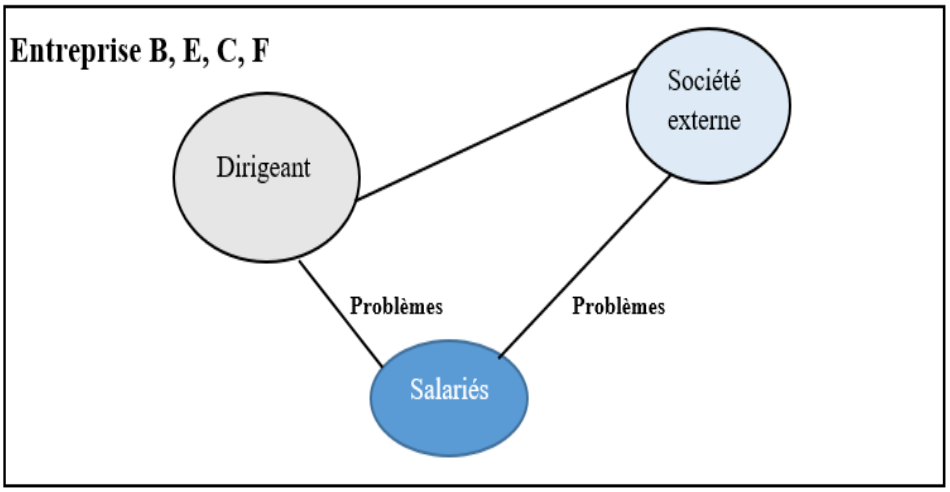
Les entreprises **D, G** et **H**, qui ont des niveaux respectifs en sécurité moyens, forts, faibles, ont un référent informatique. Dans les trois cas, ces derniers ne sont pas des informaticiens à la base. Les salariés de ces entreprises remontent les problèmes liés à la sécurité à la direction et/ou au référent informatique.

Enfin, les entreprises **B, E, C** et **F**, niveaux moyens (B, E) et faibles (C, F) en sécurité, la gestion de leurs informatiques passe par une société externe. Les salariés de ces quatre entreprises ont tendance à informer leurs dirigeants en premier lieu en cas de problèmes et la société externe, en deuxième lieu.

Représentation de la gestion de la sécurité des SI dans les entreprises







Retour sur les caractéristiques des entreprises

Entreprise	Niveau de sécurité	Taille	Chiffre d'affaires	Secteur d'activité
A	Fort	80	35.074.500	Commerce de gros
G		250	13.389.000	Tri et recyclage, blanchisserie, atelier paysage
B	Moyen	35	12.795.200	Commerce de gros
D		70	20.000.000	Transformation et conservation
E		30	2.138.400	Travaux d'étanchéification
H	Faible	20	1.011.500	Transformation et conservation de légumes
C		40	500.283	Aménagement paysager
F		19	2 .029.300	Commerce de détails

Tableau 45 : Retour sur les caractéristiques des entreprises selon leurs niveaux de SSI

Si nous comparons les caractéristiques des entreprises selon leur niveau de sécurité, nous trouvons que les entreprises qui ont le plus fort niveau de sécurité **(A, G)** sont de grandes tailles en termes d'effectifs par rapport les autres : 80 salariés pour l'entreprise A et 250 pour l'entreprise G. Les entreprises qui ont un niveau moyen de sécurité **(B, D, E)** ont des tailles moyennes par rapport aux autres, à l'exception de l'entreprise D qui elle, contient 70 salariés. Enfin, les entreprises qui ont un niveau faible de sécurité **(H, F, C)** ont les plus petites tailles (19 et 20 salariés), à l'exception de l'entreprise C qui elle, a une taille moyenne de 40 salariés mais avec un chiffre d'affaires le plus faible entre toutes les entreprises.

En ce qui concerne le secteur d'activité, nous ne pouvons pas faire une comparaison, étant donné que les entreprises étudiées appartiennent à des secteurs d'activités proches, nous n'avons pas des entreprises qui appartiennent au secteur de l'informatique, la télécommunication etc., qui sont généralement des secteurs plus sensibles à la sécurité.

La figure suivante représente le dendrogramme de l'entreprise regroupée par similarité d'attributs, à savoir : la taille, la forme juridique, le secteur d'activité ainsi que le chiffre d'affaires.

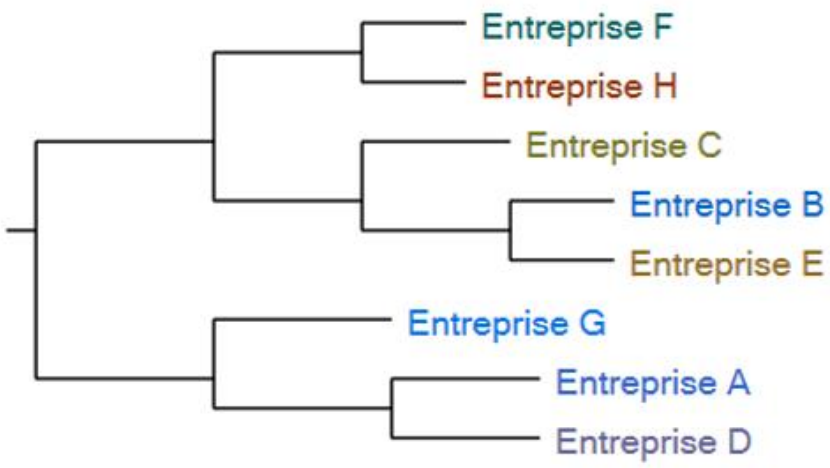


Figure 34 : Cas regroupés par similarité de valeur d'attributs (Taille, forme, secteur, CA)

Nous avons deux grosses branches : la première avec les entreprises de petites et moyennes tailles (F, H, C, B et E) et la deuxième avec les entreprises de plus grandes tailles (G, A et D).

2. Vers une typologie des utilisateurs du SI

Ce deuxième titre de notre analyse va dans un premier lieu représenter la culture sécurité des salariés interrogés (2.1). Dans un second lieu, nous mettons la lumière sur les comportements liés à la sécurité de ces mêmes salariés (2.2). Notre objectif dans cette section est de présenter une classification des salariés selon leurs niveaux de culture sécurité et de faire le lien entre culture sécurité et comportements sécuritaires.

2 .1 La culture sécurité des utilisateurs du SI

L'élément d'analyse : ''la culture sécurité'', est composé de trois sous-éléments qui sont déjà identifiés dans le cadre théorique de notre recherche, à savoir : la **propriété de sécurité**, la **conscience** et la **conformité** qui seront développés dans les sous-éléments suivants.

2.1.1 Propriété de sécurité

Nous allons présenter les résultats sous forme de tableaux et ensuite, chaque tableau sera commenté :

Sous thème Intérêt pour la sécurité	Entreprise concernée	Personnes concernées	*Exemples de verbatim*
Intéressé	A(3), B (3), G (4), D (1), H (1)	Catherine, Jennyfer, Pierre, Gaétan, Marie-Laure, Maxime, Brigitte, Marie, Mélissa, Pol-Lou, Sabine, Julian	*''Bah oui, c'est important quand même, c'est savoir faire attention à ce qu'on dit, de savoir utiliser notre ordinateur de manière très cadrée quand même''* (Jennyfer)
			''Je ne suis pas experte, mais je pense que c'est précieux de s'y intéresser parce que pour avoir déjà vécu des situations dans mes expériences professionnelles, par exemple vous ouvrez un mail le virus arrive, ça met un tas de PC en rideau. Donc je pense qu'il faut être très (très) prudent quand on utilise l'informatique par rapport à la sécurité voilà !'' (Brigitte)
Moins intéressé	C(3), H(3), E(2), F(2)	Bénédicte, Christine, Danielle, Franck, Jonathan, Robin, Marie Sandrine, Maïwenn,	*''Pas du tout ! Parce que je me sens pour l'instant pas trop concerné. Franchement non ce n'est pas un sujet qui m'intéresse pas je n'ai pas trop d'habitudes. Après maintenant il y a des personnes qui sont compétentes dans ce domaine-là pour faire face à ce genre de problèmes, donc je leur fais confiance.''* (Bénédicte)
			''ce n'est pas un domaine qui m'intéresse'' (Robin)

Tableau 46 : Intérêt exprimé pour la sécurité des SI par les utilisateurs

Nous trouvons 3 salariés de l'entreprise A qui expriment un intérêt pour le sujet de la sécurité des SI, 4 salariés de l'entreprise **G**, 3 salariés de l'entreprise **B**, mais aussi 1 salarié de l'entreprise **D,** ce qui représente 100% des salariés de ces entreprises qui s'intéressent à la sécurité. Ensuite, une seule personne de l'entreprise **H** exprime un intérêt pour la sécurité, ce qui représente 25%, soit un quart. Pour les salariés qui sont moins intéressés à la sécurité, nous

trouvons 3 salariés de l'entreprise **C,** ce qui représente 100%, puis 2 salariés de l'entreprise **H** et 2 de l'entreprise **E** et un salarié de l'entreprise **F.** Donc, les salariés qui expriment un intérêt à la sécurité le plus élevé par rapport aux autres appartiennent aux entreprises qui ont le plus fort niveau de sécurité, comme les entreprises A, G, B et D. Les salariés qui expriment un intérêt faible ou qui ne s'intéressent pas à la sécurité appartiennent aux entreprises qui ont les plus faibles niveaux de sécurité (H, C, F, E).

Sous-thème Responsabilité envers la sécurité	Entreprise concernée	Personnes concernées	*Exemples de verbatim*
Je ne suis pas responsable	C (1)	Fabien	‘*’A aucun moment je me sens responsable de la sécurité informatique clairement voilà !’’* (Fabien)
Je suis responsable en partie	H (2), E(2), G(1), F(1), C(1), D (1)	Christine, Julian, Danielle, Franck, Brigitte, Maïwenn, Robin, Sabine	*’’Oui, je suis responsable de la sécurité à mon niveau et à ce que je fais au sein de l'entreprise au niveau de la communication, je suis libre sur les réseaux sociaux de mettre ce que je veux. Même au niveau de la protection des données, qu'on n'a jamais eu d'attaques spécifiques. Mais après, chacun est responsable de ce qu'il fait.’’* (Maïwenn)
			’’Un peu quand même oui ! Si je ne divulgue pas certaines choses, ça reste quand même confidentiel ! Il ne faut pas que n'importe qui puisse y avoir accès.’’ (Sabine)
Je suis responsable	A (3), G(2) B (1), C (1),	Catherine, Pierre, Jennyfer, Mélissa, Pol-Lou,	*’’je reçois un mail, je suis quand même responsable de l'ouvrir ou pas… Donc partant de là, oui il y'a encore de la responsabilité de ne pas divulguer toutes sortes d'informations de droite et de gauche et sous n'importe quel moyen’’* (Catherine)

		Maxime, Jonathan	*''Oui ! Surtout où on est dans notre service ressources humaines paye c'est vrai qu'on gère beaucoup les informations personnelles des salariés. Donc je pense qu'on a quand même intérêt à faire attention à ce qu'on fait, parce que ça ne concerne pas que nous : ça concerne aussi tous les salariés de l'entreprise, donc je pense qu'on nous demande aussi d'être vigilants s'ils voulaient encore plus maintenant avec les nouvelles lois, le RGPD tout ce qui va avec. Je pense qu'on est responsable. En tout cas, surtout dans mon service, je trouve après que nous on doit faire très attention !''* (Mélissa)

Tableau 47 : Degré de responsabilité envers la sécurité, exprimé par les utilisateurs

Parmi les salariés qui se sentent responsables de la sécurité SI de leurs entreprises, 3 salariés de l'entreprise **A** (100%), 2 de l'entreprise **G**, 1 de l'entreprise **B** et 1 de l'entreprise **C.** Pour les salariés qui pensent qu'ils sont responsables en partie de la sécurité, on en trouve 2 de l'entreprises **H** et **E,** et un salarié dans chacune des entreprises **G, D, F, C.** Nous pouvons également trouver un salarié de l'entreprise **C**, qui ne se sent **pas du tout responsable** de la sécurité des SI de son entreprise.

Nous remarquons que plus l'entreprise a un niveau de sécurité élevé et sa direction est sensible à la sécurité, plus les utilisateurs se sentent responsable à leur tour de la sécurité des SI de leurs entreprises.

Sous thème Qui est responsable de la sécurité ?	**Entreprise concernée**	**Personnes concernées**	***Exemples de verbatim***
Je ne sais pas	C(1)	Robin	*"Je ne sais pas du tout, après je ne sais pas qui gère les réseaux, souvent c'est peut-être des entreprises extérieures qui ont plus de lien avec la sécurité, je ne sais pas !''* (Robin)
C'est la responsabilité de la direction	H(4), A(1), C(1), E(1), F(1), G(1)	Bénédicte, Brigitte, Catherine,	*''Alors, pour moi cette sécurité appartient à la direction, et en lien avec le service informatique''* (Catherine)

/Service informatique/ Responsable informatique		Christine, Danielle, Fabien, Marie, Sandrine, Julian	*''Le gérant, parce qu'on est une petite entreprise, on n'a pas de service informatique. Donc pour moi c'est de la direction pour la mise en place d'antivirus ou autre''* (Sandrine)
Tout le monde est responsable	G(3), B(3), A(2), D(1), E(1) F(1), C(1)	Franck, Gaétan, Jennyfer, Jonathan, Maïwenn, Marie, Marie-Laure, Maxime, Mélissa, Pierre, Pol-Lou, Sabine	*''La sécurité et confidentialité des données ! C'est un peu chacun sur son poste ou peut être une politique générale. Après chacun individuellement prend ses responsabilités sur son poste sous la responsabilité de tout le monde''* (Franck)
			''Toutes les personnes qui utilisent le réseau informatique, chacun est responsable de ce qu'il fait et ce qu'il donne comme information.'' (Maïwenn)

Tableau 48 : Qui est responsable de la sécurité des SI de l'entreprise (Avis des utilisateurs)

Quand nous avons demandé aux utilisateurs qui était la personne responsable de la sécurité des SI de l'entreprise, un parmi eux a répondu qu'il ne savait pas (entreprise **C**), **4** salariés de l'entreprise **H** (100%) pensaient que c'était la responsabilité de la direction**,** un salarié de l'entreprise **A** pensaient que c'était la responsabilité du service informatique. Un seul salarié pour l'entreprise **C, E, F** et **G** estimait que c'était la responsabilité de la direction et/ou du responsable informatique.

Trois salariés de l'entreprise **G**, **3** de l'entreprise **B**, **2** de l'entreprise **A** et **1** pour chacune des entreprises **D, E, F, et C** pensent que la sécurité des SI est la responsabilité de tout le monde dans l'entreprise et que chacun sur son poste peut contribuer au sein de la sécurité de son entreprise. Nous remarquons que les personnes qui pensent que la sécurité des SI est la responsabilité de tout le monde de l'entreprise appartiennent majoritairement aux entreprises qui ont les plus hauts niveaux de sécurité **(A, G et B)** par rapport aux autres.

2.1.2 Conscience

Sous thème Connaissances des mesures prises	**Entreprise concernée**	**Personnes concernées**	***Exemples de verbatim***
Pas de connaissances	H(2), C(2), E(1), F(1), G(1), B(1), D(1)	Brigitte, Bénédicte, Christine, Fabien, Jonathan, Franck, Marie, Marie-Laure, Sabine	*''Je ne sais pas ! Je crois qu'il y'a quelque chose. Je sais plus, je ne sais plus je ne peux pas trop vous dire non !''* (Christine)
			''Je ne sais pas quelles mesures sont mises en place. Je ne peux rien dire là-dessus.'' (Fabien)
Connaissances	A(3), G(3), B(2), E(1), F(1), C(1), H(2)	Catherine, Danielle, Gaétan, Jennyfer, Maïwenn, Marie, Maxime, Mélissa, Pierre, Pol-Lou, Robin, Sandrine, Julian	*Oui, oui, on travaille en collaboration avec une entreprise d'informatique qui intervient régulièrement et c'est un sujet pris à bras le corps par l'entreprise puisque ça été notifié par le nôtre ! On a fait l'état des lieux par notre assurance et qui a relevé des points de faiblesses ça nous a fait partir un peu et maintenant on a relevé tous les seuils de sécurité, on est beaucoup plus vigilants sur ce qui se passe au niveau informatique. C'est vrai, on fait attention oui !''* (Gaétan)

Tableau 49 : Connaissance des mesures sécuritaires déjà prises dans l'entreprise

Pour la connaissance des mesures de sécurité déjà en place dans l'entreprise, la majorité des salariés qui ne connaissent pas les mesures de sécurité en place appartient aux entreprises qui ont les niveaux les moins faibles en sécurité **(H, C, F),** à l'exception d'un seul salarié qui appartient à une entreprise de bon niveau de sécurité **(G)**.

Pour les salariés qui connaissent les mesures sécuritaires mises en place par leurs directions. La plupart d'entre eux appartiennent aux entreprises qui ont les plus hauts niveaux de sécurité **(A, G, B),** à l'exception de quelques salariés qui travaillent dans les entreprises avec un faible niveau de sécurité **(C, H, F).**

Sous thème Connaissances d'autres types de menaces	**Entreprise concernée**	**Personnes concernées**	***Exemples de verbatim***
Pas de connaissances	H(4), C(2), F(2), E(2), B(1), G(2)	Bénédicte, Brigitte, Christine, Danielle, Fabien, Franck, Julian, Maïwenn, Marie, Marie, Marie-Laure, Robin, Sabine	*''Non je ne connais pas !''* (Danielle)
			''Non, non. Honnêtement non'' (Fabien)
Connaissances	A(3), B(2), G(2), D(1)	Catherine, Jennyfer, Gaétan, Jonathan, Maxime, Mélissa, Pierre, Pol-Lou, Sabine	*''Mais ça peut venir de l'interne et pas forcément d'une menace extérieure à l'entreprise quoi ! Après il y'a les virus, les mails où il y'a des fichiers où il faut cliquer dessus puis on sera infecté entre guillemet par un virus''* (Jennyfer)

Tableau 50 : Connaissance des types de menaces et risques potentiels liés à la sécurité SI

Les utilisateurs qui donnent des exemples de menaces qui peuvent nuire les SI d'une entreprise sont des salariés au sein des entreprises qui ont un niveau de sécurité plus élevé que les autres **(A, G, B, D)**, et inversement : les salariés qui ne savent pas ou ne donnent pas des exemples de menaces appartiennent aux entreprises qui ont les plus faibles niveaux de sécurité **(H, C, F)**, sauf quelques salariés **(G(1), B(1))** que nous tentons de comprendre ou de leur expliquer les raisons derrière ces comportements dans les parties suivantes.

Sous thème Comment se protéger	Entreprise concernée	Personnes concernées	*Exemples de verbatim*
Pas de connaissances	C(1), B(1)	Fabien, Marie-Laure	*''Non je ne sais pas !''*(Marie-Laure)
		Bénédicte, Brigitte, Catherine, Christine, Danielle, Franck,	*''Via un antivirus via les mots de passe. Je ne vois pas d'autre solution''* (Julian)

Connaissances faibles	H(4), G(3), E(2), C(2), A(1), D(1)	Jonathan, Julian, Marie, Pol-Lou, Robin, Sabine, Sandrine	*''Mettre en place des logiciels, des antivirus pour protéger au maximum les données par des mots de passe, Voilà !''* (Sandrine)
Connaissances	A(2), F(2), B(2), G(1)	Gaétan, Jennyfer, Maïwenn, Marie, Maxime, Mélissa, Pierre	*''Je pense que déjà mettre des systèmes de sécurité informatique. Mais je ne suis pas sûre que ça serve à bien grand-chose ! Voilà être vigilant au maximum de ce qu'on fait sur Internet là où on va sur les sites, faire attention aux spams ou mails indésirables. Après, je vous dirai qu'il y arrive quand même quoi ! Être au maximum vigilant mais on n'est pas à l'abri, on n'est jamais bien à l'abri à 100% moi je pense !''* (Mélissa)

Tableau 50 : Savoir comment se protéger contre les menaces et les risques

Deux salariés ne savent pas comment se protéger contre les menaces liées aux SI, un salarié de l'entreprise **C** (faible niveau de sécurité), et un autre de l'entreprise **B** (niveau de sécurité moyen). D'autres ont des connaissances faibles qui se limitent à citer l'utilisation des anti-virus ou des mots de passe. Pour ceux qui connaissent plus que les autres les moyens de protection et le fait de penser à être vigilant et que les menaces ne peuvent pas être que de l'extérieur de l'entreprise mais de l'intérieur également, ces salariés appartiennent aux entreprises les plus sensibles à la sécurité **(A, G, B)**, à l'exception de deux salariés de l'entreprise **F**, qui est d'un faible niveau de sécurité.

Faire face à des problèmes de sécurité

La plupart des utilisateurs (16 utilisateurs) pensent qu'ils ne sont **pas capables** de faire face à des problèmes liés à la SSI, mais plutôt de faire recours à quelqu'un d'autre comme le service informatique ou la direction. Tel que le salarié de l'entreprise H : *« Non, parce qu'en fait je ne sais pas je ne connais pas les moyens, je ne saurais pas comment réagir je ne saurais pas où aller, comment contrer ça. Du coup je me réfère à ma direction directement. Je prendrai pas d'initiative si je vois une menace venir, mais je n'agirai pas toute seule quoi !* » (Sandrine). Il y'a ceux qui pensent qu'ils n'ont pas les compétences pour faire face à des problèmes de la

SSI, « *Non ! Parce que je n'y connais rien ! Après je ne sais pas, peut être, on n'est pas compétents pour régler des problèmes !* » (Franck, entreprise E), « *Je ne sais pas si j'ai des compétences je n'ai pas de compétences là-dessus ! J'ai été informé mais pas de compétences* » (Pol-Lou, entreprise G).
Un seul utilisateur pense qu'il est capable de **faire face, mais en partie** : « *Comme je vous disais finalement faire face directement non ! Mais si c'est pour un mail entrant qui m'interroge, je suis prête ! Si j'ai personne pour me dire que voilà, ce qui me semble quand même étrange comme ça, n'a rien à voir avec mon travail ou mes tâches je suis prête comme ça je suis sûre que, si ça me parle pas ! Mais sinon faire face non après à côté je ne suis pas informaticienne je ne vais pas pouvoir voilà !* » (Marie, entreprise G)

Deux utilisateurs de l'entreprise A et de l'entreprise B croient qu'ils peuvent réagir eux-mêmes en cas de problèmes : « *Je dirais oui, parce que dès quelque chose qui sort de l'ordinaire on se renseigne, tout simple c'est un courrier quand on le reçoit, disons que j'ai un compte bancaire ou j'appellerai les fournisseurs pour savoir si effectivement, il y a un souci. Après je dirai qu'une chose peut être différente, imaginons que j'ouvre un mail frauduleux par inadvertance, qu'il y a un souci dessus et que chef informaticien n'est pas là, qu'est-ce que je fais je ne sais pas ! Peut-être que j'enverrai un mail au chef informaticien qui puisse regarder, j'avais retiré aussi ma direction, ce genre de choses. Je pense, oui je serai capable de réagir* » (Pierre, entreprise A).

2.1.3 Conformité

Pour le sous-thème conformité, nous avons pris en compte l'aspect de la formation, si les utilisateurs ont eu une formation liée à la SSI, ou non. Parmi tous les utilisateurs, 3 d'entre eux qui appartiennent à l'entreprise **A** (Jennyfer, Pierre, Catherine) ont reçu une formation à la sécurité. Une seule utilisatrice de l'entreprise **B** (Marie-Laure) a reçu une formation à l'RGPD que nous considérons liée à la sécurité des informations.

Voici l'avis des utilisateurs de l'entreprise **A,** vis-vis la formation qu'ils ont reçue : « *Et oui comme j'ai dit c'est vrai que ça change la donne pour la création des mots de passe, donc c'est ça surtout. Ça sensibilise aussi dans le fond, surtout qu'on sait quand peut croiser toute sorte de chose quand on reste connectés sur internet mais ça nous sensibilise un petit peu plus en fait. Ils avaient parlé du dark web en particulier ça je ne connaissais pas du tout et après j'ai entendu parler d'internet gris ! Je me suis dit ah y a le gris aussi ! »* (Catherine)

« *Oui, oui parce que j'avais par exemple le même mot de passe pour mon compte bancaire, ma boite mail et tout ça et du coup j'ai changé. J'ai changé, j'ai quand même des différents* »

« *Pour le coup moi, avec une simple formation on nous a montré les dégâts qui pourraient nous faire ce type de problèmes, ça m'a fait prendre conscience qu'il faut faire attention et qu'il faut changer les mots de passe et ne pas avoir le même partout et pleins de choses d'autres* ». (Jennyfer)

« *Joker sur cette question je devrais changer les codes d'accès. Plus souvent vous trouvez des codes d'accès un peu plus compliqués que ce que j'ai. J'avoue que maintenant les sites vous obligent à mettre des codes de rallonge avec un signe d'être. C'est vrai que de ce côté-là non, je n'ai pas fait trop d'efforts parce que je trouve que ça fait trop de codes à retenir. J'essaie de trouver les codes simples alors généralement je dis bien généralement au point de vue du travail, il n'y a pas de code personnel qui pourrait être lié à ma famille ou autre.* » (Pierre).

Pour la formation à l'RGPD, voilà le retour de l'utilisateur : « *Oui alors, une formation sur l'RGPD pour mettre en place les procédures, ce n'est pas encore fait donc ! Après on doit mettre en place des registres de sécurité sur les données voilà ! Mais ce n'est pas encore fait donc je ne me rends pas compte des procédures qu'on a ! Donc il va falloir mettre des registres pour bien connaître le système et oui j'ai retenu ça et la responsabilité est du chef de l'établissement* » (Marie-Laure). Donc, l'utilisatrice de l'entreprise B, ne retient pas grand-chose de la formation sur l'RGPD puisqu'elle vient d'être mise en place.

Estimation de la culture sécurité de chaque utilisateur

Dans cet élément, nous allons estimer le niveau de la culture sécurité des utilisateurs au travers des matrices en se référant à notre guide d'entretien et plus précisément, les questions qui concernent la culture sécurité constituée de : propriété de sécurité, conscience et conformité. L'échelle de notation de chaque sous-thème est la suivante :

Intérêt pour la sécurité

0 : Non intéressé
1 : Intéressé
2 : Tout le monde est responsable

Qui est responsable

0 : Je ne sais pas
1 : Responsabilité de la direction/informatique

Connaissance de mesures prises/Autres types de menaces

0 : Pas de connaissances
1 : Connaissances

Comment se protéger :

0 : Pas de connaissances
1 : Connaissances faibles
2 : Connaissances

Participation à une formation

0 : Pas de participation
1 : Participation faible
2 : Participation

Entreprise A	Catherine	Jennyfer	Pierre
Propriété de sécurité			
Intérêt pour la sécurité	1	1	1
Qui est responsable	1	2	2
Conscience			
Connaissance de mesures prises	1	1	1
Autres types de menaces	1	1	1
Comment se protéger	1	2	2
Conformité			
Participation à une formation	2	2	2
Total culture sécurité	7	9	9

Matrice 4 : Estimation de la CSSI des utilisateurs de l'entreprise A

Entreprise B	Marie-Laure	Maxime	Gaétan
Propriété de sécurité			
Intérêt pour la sécurité	1	1	1
Qui est responsable	2	2	2
Conscience			
Connaissance de mesures prises	0	1	1
Autres types de menaces	0	1	1
Comment se protéger	0	1	1
Conformité			
Participation à une formation	1	0	0
Total culture sécurité	4	6	6

Matrice 5 : Estimation de la CSSI des utilisateurs de l'entreprise B

Entreprise C	Fabien	Jonathan	Robin
Propriété de sécurité			
Intérêt pour la sécurité	0	0	0
Qui est responsable	1	2	0
Conscience			
Connaissance de mesures prises	0	1	1
Autres types de menaces	1	1	0
Comment se protéger	0	1	1
Conformité			
Participation à une formation	0	0	0
Total culture sécurité	2	5	2

Matrice 6 : Estimation de la CSSI des utilisateurs de l'entreprise C

Entreprise D	Sabine
Propriété de sécurité	
Intérêt pour la sécurité	1
Qui est responsable	2
Conscience	
Connaissance de mesures prises	0
Autres types de menaces	1
Comment se protéger	1
Conformité	
Participation à une formation	0
Total culture sécurité	5

Matrice 7 : Estimation de la CSSI des utilisateurs de l'entreprise D

Entreprise E	Danielle	Franck
Propriété de sécurité		
Intérêt pour la sécurité	0	0
Qui est responsable	1	2
Conscience		
Connaissance de mesures prises	1	1
Autres types de menaces	0	0
Comment se protéger	1	1
Conformité		
Participation à une formation	0	0
Total culture sécurité	3	4

Matrice 8 : Estimation de la CSSI des utilisateurs de l'entreprise E

Entreprise F	Marie	Maïwenn
Propriété de sécurité		
Intérêt pour la sécurité	0	0
Qui est responsable	1	2
Conscience		
Connaissance de mesures prises	0	1
Autres types de menaces	0	0
Comment se protéger	1	1
Conformité		
Participation à une formation	0	0
Total culture sécurité	2	4

Matrice 9 : Estimation de la CSSI des utilisateurs de l'entreprise F

Entreprise G	Brigitte	Mélissa	Marie	Pol-Lou
Propriété de sécurité				
Intérêt pour la sécurité	1	1	1	1
Qui est responsable	1	2	2	2
Conscience				
Connaissance de mesures prises	0	1	1	1
Autres types de menaces	0	1	0	1
Comment se protéger	1	2	1	1
Conformité				
Participation à une formation	0	0	0	0
Total culture sécurité	3	7	5	6

Matrice 10 : Estimation de la CSSI des utilisateurs de l'entreprise G

Entreprise H	Bénédicte	Christine	Sandrine	Julian
Propriété de sécurité				
Intérêt pour la sécurité	0	0	0	1
Qui est responsable	1	1	1	1
Conscience				
Connaissance de mesures prises	0	0	1	1
Autres types de menaces	0	0	0	0
Comment se protéger	1	1	1	1
Conformité				
Participation à une formation	0	0	0	0
Total culture sécurité	2	2	3	4

Matrice 11 : Estimation de la CSSI des utilisateurs de l'entreprise H

Après l'évaluation de la culture sécurité de chaque salarié, nous allons classifier les salariés en trois catégories :

Niveau 1 : Faible niveau de culture sécurité (Couleur blanche)

Niveau 2 : Moyen niveau de culture sécurité (Couleur gris clair)

Niveau 3 : Fort niveau de culture sécurité (Couleur gris foncé)

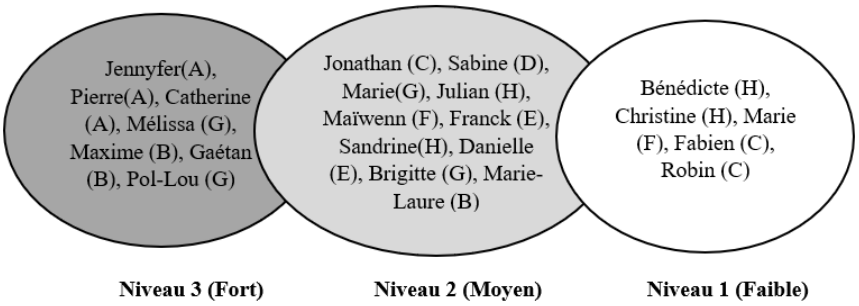


Figure 35 : Classification des utilisateurs selon leurs niveaux de CSSI

2.2 Comportements liés à la sécurité, réalisés par les utilisateurs du SI

Dans cet élément, nous allons estimer le niveau des comportements liés à la sécurité comme la fréquence du changement des mots de passe, la robustesse des mots de passe choisis ainsi que la sauvegarde des données par les utilisateurs. L'échelle de notation donc est la suivante :

Changement de mot de passe

0 : Jamais
1 : Pas souvent
2 : Quand c'est demandé
3 : Souvent

Référence à des éléments personnels

0 : Réfèrent
1 : Réfèrent et je sais que ce n'est pas bien
2 : Réfèrent mais difficile à déterminer
3 : Ne réfèrent pas

Sauvegarde des données

0 : Pas de sauvegardes
1 : Sauvegardes manuelles pas souvent
2 : Sauvegardes automatiques pas souvent
3 : Sauvegardes manuelles régulières
4 : Sauvegardes automatiques chaque semaine
5 : Sauvegardes automatiques chaque jour

Entreprise A	Catherine	Jennyfer	Pierre
Changement de mot de passe	2	3	2
Référence à des éléments personnels	2	2	3
Sauvegarde des données	5	5	5
Total comportement sécuritaire	9	10	10

Matrice 12 : Estimation du niveau de comportements liés à la SSI des utilisateurs de l'entreprise A

Entreprise B	Marie-Laure	Maxime	Gaétan
Changement de mot de passe	1	1	1
Référence à des éléments personnels	3	3	3
Sauvegarde des données	4	4	4
Total comportement sécuritaire	8	8	8

Matrice 13 : Estimation du niveau de comportements liés à la SSI des utilisateurs de l'entreprise B

Entreprise C	Fabien	Jonathan	Robin
Changement de mot de passe	0	0	0
Référence à des éléments personnels	0	3	0
Sauvegarde des données	1	1	1
Total comportements relatifs à la sécurité	1	4	1

Matrice 14 : Estimation du niveau de comportements liés à la SSI des utilisateurs de l'entreprise C

Entreprise D	Sabine
Changement de mot de passe	1
Référence à des éléments personnels	3
Sauvegarde des données	4
Total comportements relatifs à la sécurité	8

Matrice 15 : Estimation du niveau de comportements liés à la SSI des utilisateurs de l'entreprise D

Entreprise E	Danielle	Franck
Changement de mot de passe	0	0
Référence à des éléments personnels	2	0
Sauvegarde des données	4	4
Total comportements relatifs à la sécurité	6	4

Matrice 16 : Estimation du niveau de comportements liés à la SSI des utilisateurs de l'entreprise E

Entreprise F	Marie	Maïwenn
Changement de mot de passe	2	1
Référence à des éléments personnels	1	3
Sauvegarde des données	2	3
Total comportements relatifs à la sécurité	5	7

Matrice 17 : Estimation du niveau de comportements liés à la SSI des utilisateurs de l'entreprise F

Entreprise G	Brigitte	Mélissa	Marie	Pol-Lou
Changement de mot de passe	1	2	1	1
Référence à des éléments personnels	0	2	1	1
Sauvegarde des données	5	5	5	5
Total comportements relatifs à la sécurité	6	9	7	7

Matrice 18 : Estimation du niveau de comportements liés à la SSI des utilisateurs de l'entreprise G

Entreprise H	Bénédicte	Christine	Sandrine	Julian
Changement de mot de passe	2	0	2	0
Référence à des éléments personnels	0	0	3	3
Sauvegarde des données	2	2	2	2
Total comportements relatifs à la sécurité	4	2	7	5

Matrice 19 : Estimation du niveau de comportements liés à la SSI des utilisateurs de l'entreprise H

Après l'évaluation de la culture sécurité de chaque salarié, nous allons classifier les salariés en trois catégories :

Niveau 1 : Faibles comportements liés à la sécurité (Couleur Blanche)

Niveau 2 : Moyens comportements liés à la sécurité (Couleur gris clair)

Niveau 3 : Forts comportements liés à la sécurité (Couleur gris foncé)

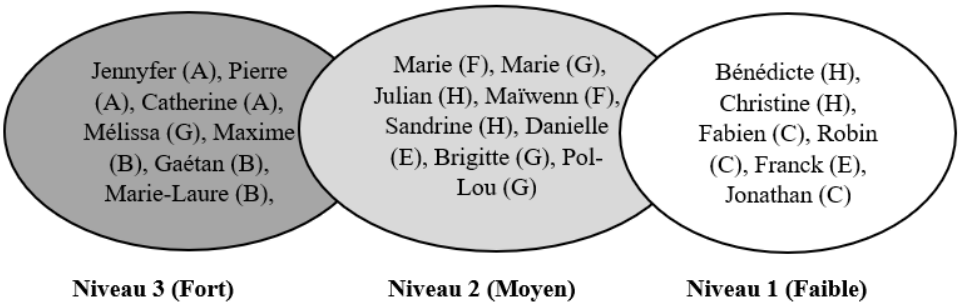


Figure 36 : Classification des utilisateurs selon leurs niveaux de comportements relatifs à la SSI

Les principaux freins aux comportements liés à la sécurité exprimés par les utilisateurs :

Changement des mots de passe	Total	Exemple verbatim
Par peur d'oublier le mot de passe	4	*'' Euh, une fois par an je ne peux pas dire plus oui, même pas une fois par an moins que ça je pense, c'est par soucis d'en pouvoir se rappeler quoi !''* (Gaétan)

Tableau 51 : Premier frein aux comportements relatifs à la SSI

Mots de passe qui réfèrent à des éléments personnels	Total	Exemple verbatim
Facile à retenir	3	*''Parfois il y'a des mots de passe sécurisés où on met des majuscules mais dans la plupart du temps je mets des trucs facile à retenir''.* (Franck) *''Après ce n'est pas forcément facile à retenir et on se retrouve avec des listes comme je disais tout à l'heure avec plein de mots de passe''* (Marie)

Tableau 52 : Deuxième frein aux comportements relatifs à la SSI

Synthèse de la section 2

Dans cette section, nous avons présenté les résultats de notre étude de cas réalisée au sein de huit PME. En se basant sur ces résultats, nous avons pu classifier les PME selon leur niveau de maturité, en matière de sécurité des SI et les utilisateurs des SI selon leur niveau de culture sécurité et de leurs comportements liés à la sécurité. Cette classification va nous permettre de faire le lien entre les catégories des PME et les catégories des utilisateurs et de discuter ensuite nos orientations de recherche au niveau du chapitre suivant (Chapitre 4).

Conclusion du chapitre 3

Tout au long de ce chapitre, nous avons eu l'occasion d'expliciter le design de notre recherche en nous intéressant tant aux questions épistémologiques que méthodologiques dont nous rappelons les grandes lignes :

-Notre posture épistémologique se veut interprétativiste dans la mesure où nous interprétons la réalité à partir des représentations des acteurs ;

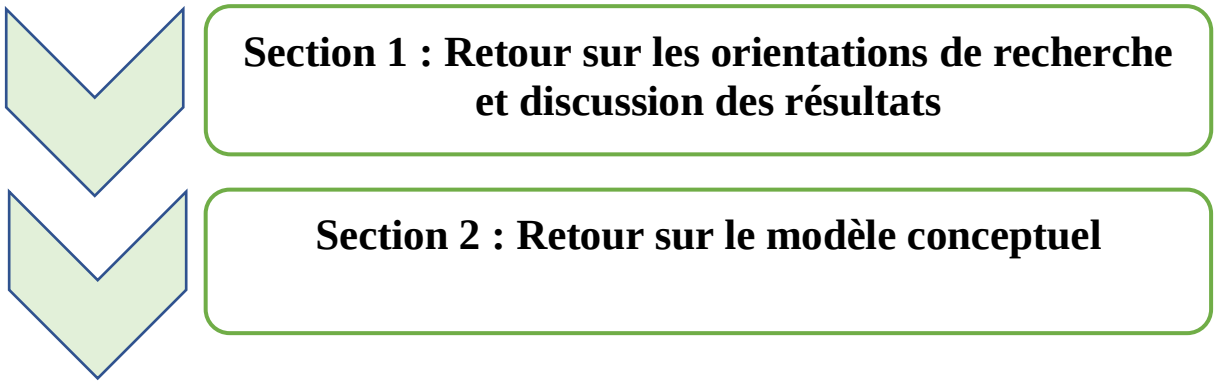
-La méthodologie utilisée est qualitative à travers l'étude des cas de PME ;

-Notre démarche est abductive, nous procédons ainsi à des allers et retours entre théorie et terrain.

Ensuite, nous avons présenté nos résultats de l'étude qualitative, en procédant à une typologie des PME étudiées et une typologie des utilisateurs selon leur culture et comportements de sécurité. Au niveau du chapitre suivant, nous allons discuter les résultats et examiner nos orientations de recherche.

Chapitre 4 : Examen des orientations de recherche et discussion des résultats

Au niveau de la première partie de notre travail et plus précisément dans le second chapitre, nous avons proposé un modèle conceptuel de la culture sécurité avec quatre principales orientations qui doivent être vérifiées à travers notre étude terrain. Au niveau de ce chapitre, nous allons dans un premier temps examiner ces orientations de recherche et de discuter les résultats obtenus par rapports aux résultats des recherches antérieures **(Section 1)**. Ensuite, nous allons réviser suite aux résultats de notre étude qualitative le modèle conceptuel initial (issu de la littérature), pour en proposer un modèle affiné suite à l'étude qualitative **(Section 2)**.



Section 1 : Retour sur les orientations de recherche et discussion des résultats

Après l'élaboration de la typologie des entreprises et la typologie des utilisateurs, nous allons revenir au sein de cette section, à nos orientations de recherche initialement proposées, afin de les examiner en croisant les deux typologies des entreprises et des utilisateurs.

1. Orientation 1 : Les facteurs exogènes

Des facteurs exogènes comme le contexte légal ou la présence d'un prestataire informatique ou bien l'appartenance à un secteur d'activité sensible à la sécurité influencent positivement la culture sécurité SI dans la PME.

1.1 Le contexte règlementaire et légal

Parmi les entreprises qui commencent à mettre en place une procédure pour se conformer à l'RGPD (Règlement général sur la protection des données), nous trouvons l'entreprise **A** et l'entreprise **B** qui ont nommé un DPO :

DSI de l'entreprise **A,** explique *: « En règlementation RGPD, je n'ai pas trop peur, mais au moins comme ça on a un DPO mutualisé, il fallait nommer quelqu'un en interne et embaucher quelqu'un, c'est pour ça qu'on a pris un DPO en mode mutualisé aussi devient RSSI »* (Thiery)

Le directeur de l'entreprise **B** annonce *: « Tout à fait, on a pris contact avec une société qui accompagne les entreprises dans les SI et on a une personne d'un profil plutôt juridique qui nous accompagne, convenu avec elle d'un accompagnement de 4 heures, 2 X 2h. Donc, elle a déjà fait les deux premières heures pour une formation de découverte ! Qu'est-ce que l'RGPD ! Et donc on a identifié au sein des équipes une personne, ce n'est pas délégué mais un DPO, le nom officiel, c'est pour les entreprises les plus grandes mais quand même, on voulait identifier une personne référente sur le sujet »* (Jean-Luc).

Pour l'entreprise **G**, elle est en cours d'étude en ce qui concerne L'RGPD : « *Donc, on en est au début, c'est à dire que ce qu'on a prévu : moi je suis responsable de cette action en lien avec Mélissa qui s'occupe donc de la gestion du personnel et donc ce qu'on a prévu de faire est en cours. Donc on a prévu d'aller voir chacun des directeurs des trois entités, pour qu'on essaie*

ensemble de lister, ce qui paraît comme étant risqué chez lui ou plutôt et aussi quelles sont les sources d'informations du RGPD sensibles qu'il y a dans son secteur d'activité » (André)

Et pour les entreprises **D**, **E** et **F** les trois dirigeants expriment qu'ils s'assurent de la conformité des données à l'RGPD auprès de leurs prestataires et que ces derniers les rassurent qu'ils sont conformes à la réglementation.

« Oui en fait, du coup on fonctionne uniquement avec des prestataires. On s'assure que les prestataires eux, se sont bien mis à jour. Après, on n'est pas très (très) exposés puisqu'on a une carte de fidélité dématérialisée sur laquelle on n'a vraiment pas beaucoup d'informations et même rien si le client ne veut rien donner, on ne demande rien, il n'est pas obligé de nous donner son nom. Ensuite après pour les salariés tout est centralisé dans le logiciel de paye donc pareil, en fait c'est plutôt via nos prestataires qu'on s'assure que ceux-ci soient en règles » (Erwan)

« Oui, oui disant qu'on s'est assurés auprès de nos prestataires qu'on était conformes voilà, après sur la partie, on avait vérifié sur la partie personnelle on n'avait pas de choses qui étaient non conformes avec les données clients et à l'RGPD, nos logiciels étaient conformes » (Sten)

Enfin pour les entreprises **C** et **H**, nous ne trouvons aucune action de conformité à l'RGPD :

Responsable informatique de l'entreprise **H** *: « Au moment on a entendu parler, mais on n'a fait aucune action de conformité. Et on traine le plus longtemps possible à ce qu'ils nous disent quelque chose. On recueille peu de données personnelles, on est sur B to B. On a une certaine base de gens qui nous connaissent, avec qui on communique. Et voilà, on n'a pas mis un responsable RGPD, on n'a pas passé une action particulière, on a un ERP qui est capable de prendre ça en compte mais pour l'instant on s'en fiche ! »* (Bruno).

A partir de ces constats, nous remarquons que les seules entreprises qui ont commencé à engager des actions de conformité à l'RGPD et qu'elles ont nommé un référent RGPD ou un DPO, l'entreprise **A** et **B**, le niveau de culture sécurité des utilisateurs dans ces entreprises est assez élevé par rapport aux autres utilisateurs, avec 3 salariés en niveau fort pour l'entreprise **A** et 2 salariés pour l'entreprise **B**. Une recherche récente de Mourrain et Leconte (2019) montre que l'obligation de la mise en application de l'RGPD génère une charge et un coût pour l'entreprise, mais constitue une réelle opportunité pour les entreprises de types ETI ou PME, moins sensibles à la sécurité des SI que les grands groupes.

Parmi les 10 acteurs de la direction interrogés, 2 acteurs expriment leurs avis sur un accompagnement des pouvoirs publics à l'instar des chambres de commerce et d'industrie (CCI). Le dirigeant de l'entreprise **B** s'exprime de la sorte : « *Je me suis rendu en fait à la CCI, qui organisait des rendez-vous en fin de matinée de trois quarts d'heure avec des prestataires. Ce que j'ai fait et c'est suite à cette rencontre que nous avons sollicité cette entreprise de la gestion des SI qui m'a amené du coup à mettre en place la formation sur l'RGPD. Donc c'est eux qui nous accompagnent sur l'RGPD mais on n'est pas allés plus loin sur la question de sécurité. Je n'ai pas été au-delà, je pense que je vais mettre ce sujet dans mes prochains axes de travail sur la sensibilisation des équipes et de faire appel à un prestataire externe pour y prouver notre SI et notre système de sécurité* » (Jean-Luc).

Nous remarquons que suite à la participation de ce dirigeant aux rencontres organisées par la CCI, il a pris l'initiative de mettre en place une formation sur l'RGPD et de lancer des actions de conformité à l'RGPD. Donc, nous remarquons l'influence de cet organisme public (CCI) sur les dirigeants et les responsables de PME à travers des rencontres d'informations ou des formations à la sécurité des SI afin de renforcer le niveau de sécurité de leurs entreprises. Cependant, ce même dirigeant exprime un besoin d'accompagnement sur le sujet de la sécurité : « *Donc on sait que la menace est là et présente dans notre environnement. Comment l'appréhender ! Comment la maitriser ça reste un sujet ! On fait mieux aujourd'hui, j'ai le sentiment qu'il y a un chemin à faire. Oui ça m'intéresse un accompagnement aux dirigeants sur le sujet, je pense que c'est un vrai sujet actuel et encore plus de demain* » (Jean-Luc).

A son tour le responsable informatique de l'entreprise **D** exprime un manque d'accompagnement sur le sujet de la sécurité : « *J'ai été une fois à la CCI suivre une formation en une conférence sur les risques liés à l'informatique. C'est très intéressant mais derrière il n'y avait rien ! Je ne sais pas à qui me référer par rapport à ça. Dès qu'on parle de sécurité on ne sait pas à qui faire confiance en fait. C'est surtout ça qui me freine aussi* » (Gabriel).

Retour sur la littérature :

Ce constat nous permet de dire que l'Etat peut jouer un rôle important en matière de la sécurité des SI, car des lois pourraient obliger les entreprises à mettre en place les actions les plus indispensables. De plus, il y a des acteurs de la direction qui expriment un besoin d'accompagnement pour savoir quelle démarche mettre en place. Comment faire face aux risques et aux menaces ? A qui faire confiance sur le sujet de la sécurité ?

Cette influence a été mise en lumière par Dojkovski et al, (2007) dans les PME australiennes où ils mentionnent que les gouvernements (fédéraux et étatiques) peuvent jouer des rôles de soutien clés - notamment dans le contexte australien - par la distribution de brochures de sensibilisation à la SSI aux PME ainsi que la conduite de l'analyse comparative nationale de la SSI des PME. Pour aider les organisations australiennes, des exemples de scénarios de risque de sécurité peuvent être développés à partir des ressources de SSI existantes. Celles-ci peuvent être formulées en termes de protection contre la perte d'actifs, afin de mieux attirer les PME. Les initiatives devraient cibler également le contexte national. Par exemple, l'Australie a une culture de laissez-faire et donc, les brochures et autres initiatives devraient viser à répondre à cette caractéristique « d'acceptation des risques ».

1.2 Prestataires de services informatiques

Toutes les entreprises étudiées font recours à un prestataire ou une société externe qui gère leur informatique, ou bien une partie. Nous avons pu identifier les relations entre les entreprises et leurs prestataires informatiques :

Une relation de confiance avec le prestataire, comme l'expriment le responsable informatique de l'entreprise **D** et le directeur adjoint de l'entreprise **G** : « *Comme je vous le disais tout à l'heure, on n'a pas à proprement parler d'informaticiens dans l'entreprise qui a une culture d'informatique donc effectivement, on a fait le choix de ne pas multiplier en interne les personnes ressources puisque c'est un coût important aussi et donc on fait confiance au prestataire qui a un rôle important pour nous parce qu'on lui délègue notre infogérance donc on essaie de faire des points réguliers avec lui* » (André).

Une confiance limitée ou une insatisfaction vis-à-vis des prestataires, le dirigeant de l'entreprise **B** qui exprime : « *Leurs rôles aujourd'hui d'être forces de conseils, fin j'ai quelques doutes que ce rôle soit pleinement rempli, en tout cas c'est moi qui sensibilise mes interlocuteurs et je leur fais part de mes interrogations et de mes craintes à ce sujet. Et ces craintes émanent de mes échanges avec notre assureur qui est très vigilant sur ce sujet-là. Et donc, j'en parle avec eux régulièrement mais ! Par exemple, on devrait faire un test de récupération de données pour bien faire les choses aujourd'hui et ça n'a pas été fait ! Et je ne sens pas un engouement particulier de la part de notre prestataire pour réaliser ces tests et pourtant ça me rassurerait de le faire et que ça fonctionne comme il le faut. Et régulièrement,*

quand on a notre audit mené par notre assurance, c'est un sujet qui revient. Ils sont dans l'attente de la conduite de ce test de restauration de données » (Jean-Luc).

Un rôle de conseil et de support technique, cas des entreprises **C, D, G, E** et **F** :
« *Après, son rôle aujourd'hui va être plutôt quand même de support téléphonique ça oui, il a quand même un rôle important s'il y a nécessité mais ce n'est pas automatique. Tu n'es pas rentré dans un jeu de contrat premium où j'ai un gars qui vient me voir en* permanence *pour voir ce qui se passe* » (Romain).

« *Alors, son rôle est lié plus de conseils et de moyens techniques au niveau des systèmes d'information, après on a fait des vérifications des mises à jour Windows ce genre de choses c'est un peu ça son rôle à mon sens, son rôle de conseil et de propositions de moyens techniques au niveau de structure* » (Jean-Marc).

Rôle d'RSSI et DPO[29] : Pour le DSI de l'entreprise **A**, le prestataire audite l'entreprise, joue un rôle de l'RSSI et du DPO : « *On travaille avec le groupe « X » et son rôle est justement de faire les audits et de jouer le rôle de la RSSI et DPO* » (Thiery).

Relation non stable avec le prestataire : Le cas de l'entreprise **H** où son responsable informatique exprime : « *difficile de répondre parce qu'on est en train d'en changer. On avait un prestataire pendant des années et puis il est en train de se casser la gueule donc on est en train de regarder autour de nous quel prestataire il peut y avoir ! On cherche quelqu'un qui établit et qui est connu mais qui a un coût relativement modeste, on a des gros budgets sur les machines* » (Bruno).

Une entreprise sur 8 a dans le contrat avec son prestataire des clauses qui concernent la sécurité informatique (Entreprise **A**). L'entreprise **G** a une charte avec son prestataire, mais qui n'est pas actualisée depuis un moment. Les autres entreprises **B, C, D, E, F** et **H** n'ont pas de chartes ni de clauses contractuelles qui sont spécifiques à la sécurité informatique avec leurs prestataires.

Retour sur la littérature :

Ces résultats sont en cohérence avec ce que nous avons identifié au niveau de la littérature, que les prestataires de services informatiques peuvent jouer un rôle clé dans la sensibilisation à la

[29] Délégué de la protection des données

sécurité des SI, mais peuvent aussi créer un sentiment de défiance de la part de leurs clients, qui auraient l'impression de se voir proposer du matériel et des logiciels inutiles (Dojkovski et al 2007). Une étude de Lee and Larson (2009) à propos de l'influence sociale des principales parties prenantes et des variables spécifiques à la situation, tel que le soutien des fournisseurs, tient compte des écarts considérables entre les intentions d'adoption et l'adoption réelle des logiciels anti-malware[30] par les PME.

Les précédentes études d'adoption de l'informatique par les PME ont suggéré la sollicitation d'un soutien étendu des fournisseurs, y compris la présence de techniciens désignés, un accès facile à l'assistance technique et une formation périodique. Par exemple, une étude de Lee and Larson (2009) montre que plus le support des fournisseurs est attendu, plus les dirigeants des PME sont enclins à adopter un logiciel anti-malware.

1.3 Le secteur d'activité

Nous avons identifié des déclarations de trois dirigeants et une déclaration d'un salarié, qui font référence au secteur d'activité.

Le dirigeant de l'entreprise **F** (commerce de détail) déclare : « *Je n'ai rien à voler ! Plutôt que de dérober de l'information sur mon ordinateur, il suffit de me le demander et je vous donne accès à ma boite mail, je n'ai rien en fait ! Je n'ai rien de confidentiel, évidemment ce sont des choses qui peuvent intéresser la concurrence mais par curiosité en amitié ils ne feront jamais rien, c'est des accords que j'ai avec des fournisseurs, savoir si j'ai 13% ou 18% de remise ça ne va pas aller faire des miracles chez eux, ensuite en réalité je n'ai absolument rien de sensible comme informations sur les postes de travail* » (Erwan)

Le dirigeant de l'entreprise **E** (travaux d'étanchéification) exprime : « *Aujourd'hui, moi je vais me considérer comme étant purement anonyme, on n'est pas sur du stratégique, On a des données commerciales comme n'importe quelle entreprise, quelle que soit son activité. Voilà, on est dans un domaine tellement banal que finalement, je ne vais pas considérer avoir un besoin de protection premium… si jamais on vient nous faire un chantage à nos données, bon c'est*

[30] Un logiciel antimalware protège un système informatique contre les infections provoquées par les logiciels malveillants.

dupliqué dans plein d'endroits ce serait juste très chiant. Mais ce ne sera pas un drame. Peu de probabilités qu'on se fasse piquer des secrets industriels que nous n'avons pas ! » (Romain)

Le DSI de l'entreprise **A** (commerce de gros) considère que : « *Alors c'est là qu'il faut justement mettre le curseur, quelles sont les données sensibles et confidentielles de l'entreprise ? Toute entreprise a son propre curseur à mettre sur les données sensibles, un exemple : moi j'en ai discuté avec l'ancien DSI du groupe Renault, qui me disait, les données sensibles au niveau de Renault c'est uniquement le R&D tout le reste ! Une voiture ça roule ! Un volant ! Un moteur ! Le prix de vente de nos voitures tout le monde les connaît, le prix de revient de nos voitures tous nos concurrents le connaissent parce qu'ils ont exactement les mêmes. Donc, les données sensibles c'est uniquement le R&D. Nous, on fait du négoce, le prix de la matière première tous nos concurrents le connaissent, ils achètent la même matière première que nous, nos prix de vente tout le monde le connaît ! Quelle est la donnée sensible du négoce ? Y en n'a pas beaucoup, donc la donnée sensible est uniquement ce que les actionnaires ont envie de faire pour le groupe, c'est plus ça. Et donc, la transmission de données sensibles est plus orale entre les actionnaires qu'écrite ou mise dans le SI. Donc est-ce qu'on a des données sensibles et confidentielles ? La paye elle est externalisée, donc je dirai : pas vraiment ! Donc nous, on a mis le curseur à un certain niveau, on a mis en place une procédure, que si c'est du confidentiel on demande à nos actionnaires s'ils doivent faire un document XL ou Word de rajouter « Confidentiel » Il n'y a pas plus de procédures que ça » (Thiery).*

Les directeurs des entreprises **E** et **F** pensent qu'ils n'ont pas de données confidentielles et qu'ils n'ont rien à craindre, puisqu'ils ont des données ou des informations commerciales dont tout le monde peut avoir accès. Ces deux dirigeants expriment qu'ils n'ont pas besoin d'un niveau de sécurité assez élevé pour protéger leurs données.

Selon notre évaluation à partir de l'analyse de contenue et selon la typologie des entreprises réalisée, l'entreprise **E** appartient au niveau moyen de sécurité avec deux salariés d'un niveau de culture sécurité moyen et l'entreprise **F** a le plus faible niveau de sécurité, avec un salarié d'un niveau moyen de culture sécurité et un avec un niveau de culture faible. L'entreprise **E** appartient au secteur des **travaux d'étanchéification** et l'entreprise **F** au secteur de **commerce de détail**.

Le DSI de l'entreprise **A** pense qu'il faut mettre le curseur sur la définition d'une donnée sensible, et qu'au sein de l'entreprise A, ils font la distinction entre les données confidentielles

et les données commerciales ou moins confidentielles, c'est ce qu'ils adoptent comme procédure pour traiter les données au sein de l'entreprise. L'entreprise **A** est dans le secteur du **commerce de gros** et selon la typologie réalisée pour les entreprises, elle est classée la meilleure en termes de niveau de sécurité de son SI.

Le salarié de l'entreprise **B** (commerce de gros**)** exprime son avis de la manière suivante : « *Donc oui je comprends que c'est assez important ce genre de choses-là, il y a vraiment des données importantes à protéger dans l'entreprise et encore, on est qu'une entreprise agro-alimentaire, il y a des secteurs où vraiment c'est plus important, je pense vraiment totalement au nucléaire et tout ça où là pour le coup, le niveau de sécurité est très (très) impressionnant* » (Maxime).

Ce salarié fait une comparaison entre le secteur de son entreprise **B** qui est **agro-alimentaire,** où il estime que la sécurité est plus importante dans les secteurs où les données confidentielles sont plus importantes, tel que le secteur du nucléaire.

Retour sur la littérature :

A partir de ces constats et de ces verbatims, nous pouvons conclure que l'appartenance à un secteur d'activité précis peut déterminer la façon dont les données sont traitées au sein d'une PME, plus le secteur d'activité est sensible à la confidentialité des données et plus le niveau de sécurité sera important par rapport aux secteurs d'activités qui sont moins sensibles à la confidentialité de leurs données, comme le secteur de commerce. Ce constat est en cohérence avec les travaux de Dagorn et Poussing (2012), en matière de gouvernance de la SSI, qui montre que la difficulté à traduire les concepts en actions concrètes, à appartenir au secteur de l'industrie comparativement au secteur des services. Ainsi que les études qui soulignent l'importance qui peut avoir l'effet de l'activité de l'entreprise dans le domaine de la SSI, Djokovski et al (2007), Barlette (2012).

Nous n'avons pas pu détailler la différence entre les PME techniques appartenant aux secteurs de : l'informatique, télécommunications, service financier… des PME non techniques appartenant aux autres secteurs d'activité, vu que les PME étudiées appartiennent à des secteurs d'activité très proches l'un de l'autre (commerce de gros, commerce de détail, transformation et conservation, service d'aménagement…), qui sont des PME non techniques.

Donc, nous constatons l'importance du secteur d'activité dans l'étude du niveau de sécurité des SI des PME et par conséquent, dans l'étude du niveau de la culture sécurité des utilisateurs

2. Orientation 2 : Les facteurs endogènes

Des facteurs endogènes comme l'existence d'une évaluation des risques liés à la sécurité des SI ou la réalisation de formations en matière de sécurité des SI influencent positivement la culture sécurité SI de la PME.

2.1 La gestion des risques

Pour la gestion des risques lié aux systèmes d'information, nous avons basé notre évaluation sur le référentiel Cobit, qui est un référentiel de bonnes pratiques d'audit informatique et de gouvernance des systèmes d'information et plus précisément, nous avons appliqué la partie PO9 : Evaluer et gérer les risques. Suite à cette évaluation, nous avons deux entreprises (**A** et **G**) qui ont un fort niveau de gestion des risques par rapport aux autres et c'est à travers l'analyse et l'évaluation des risques pour l'entreprise **G** qu'il y a l'application d'une matrice de risque où ils évaluent le niveau de risques informatiques (fort, moyen, faible), ainsi que les mesures pour gérer les risques identifiés, le directeur nous a montré un exemple de matrice. Pour l'entreprise **A**, le DSI nous a expliqué qu'il mettait en place des matrices de risques selon les projets et surtout, pour les projets contraignants.

Ces deux entreprises mettent en place des plans d'actions comme le PCA (Plan de continuité d'activité) et le PRA (Plan de reprise d'activité) pour gérer les risques, le DSI de l'entreprise A explique : « *Donc on a mis en place un PRA, PCA, avec RTPO à 15 minutes, de fait de la réplication, on est en train de regarder pour viser le 0. Il y a des solutions maintenant qu'on a fait le choix de prendre ce PRA, PCA créés en 2017, maintenant, il existe des solutions techniques qui permettent d'avoir un RTPO à 0, je suis en train de regarder, c'est le curseur entre coût et technologie''* (Thiery). Et le directeur de l'entreprise G exprime : « *On a un bilan aussi, il y a une journée aussi PRA de simulation de reprise, un plan de reprise d'activité qui est fait tous les ans et une journée de PRA avec un débriefing »* (André).

Nous remarquons que pour ces deux entreprises **A** et **G**, le niveau de culture sécurité de leurs salariés est le plus élevé par rapport aux autres salariés. L'entreprise **A** a **trois** salariés d'un niveau de culture sécurité **fort** (100% des salariés interrogés) et pour l'entreprise **G**, nous trouvons **deux** salariés d'un niveau de culture sécurité **fort** (50% des salariés interrogés) et les **deux** autres salariés, eux, ont un niveau **moyen**.

Prenons maintenant l'entreprise **C** où nous ne trouvons aucune action pour gérer les risques liés aux SI, absence d'analyse et d'évaluation de risques ainsi que de plan d'action. Cette entreprise obtient une note de 0 sur 4 dans le volet gestion des risques SI. Si nous nous arrêtons sur le niveau de culture sécurité des salariés de cette entreprise, nous trouvons **deux** salariés avec un niveau **faible** de culture sécurité (65% des salariés interrogés) et **un** salarié avec un niveau **moyen**.
Pour le reste des entreprises (**B, D, E, F** et **H**) avec un niveau de gestion de risques moyen (1 et 2 points sur 4), leurs salariés sont classés dans les niveaux moyens et faibles de la culture sécurité, à l'exception des deux salariés de l'entreprise **B** (Maxime et Gaëtan) qui ont un niveau fort de culture sécurité - ce qui peut être expliqué par la compensation d'autres facteurs que nous cherchons à déterminer dans la suite de notre travail. -

Ces constats nous permettent de dire que plus l'entreprise analyse et évalue les risques liés aux SI et met en place des plans d'actions pour gérer ces risques, plus le niveau de la culture sécurité des utilisateurs de ces SI augmente. Cette conclusion est basée sur le fait que les entreprises **A** et **G** ont le plus fort niveau de gestion de risques. Leurs salariés ont les plus hauts niveaux de culture sécurité. Et inversement pour l'entreprise **C,** où la gestion des risques est absente les salariés ont les plus faibles niveaux de culture sécurité.

Retour sur la littérature :

Notre conclusion vient donc approuver les travaux de Djokovski et al (2007), qui ont montré que la gestion des risques par le biais des contre-mesures adéquates peut diminuer la probabilité de perte, aide la PME et ses employés à devenir capables de comprendre les potentiels dommages à la sécurité, ce qui contribue à créer une prise de conscience envers la culture SSI (étude sur des PME australiennes). Pour les plus grandes organisations Martin et Eloff (2002), Da Veiga et Eloff (2010), Alnatheer (2014) et Tolah et al (2017) ont montré cette influence comme importante pour les grandes organisations.

2.2 La formation et la sensibilisation

La seule entreprise où nous trouvons un programme de formation liée à la sécurité des SI destinée aux utilisateurs est au sein de l'entreprise **A**, où son DSI parle du contenu de cette formation de la manière suivante : « *Le contenu de la formation, c'est une formation de sensibilisation sur les risques informatiques, non seulement les risques professionnels mais*

aussi les risques personnels, parce que la sphère professionnelle et la sphère personnelle au niveau des utilisateurs, ça s'amalgame, donc il faut qu'on prenne en compte aussi leurs usages personnels dans cette formation-là, ça leur permet aussi de découvrir des choses et de stopper des choses aussi, qu'ils feraient ou qu'ils font au niveau personnel'' (Thiery)

Les trois salariés interrogés (Jennyfer, Catherine et Pierre) de l'entreprise **A** ont suivi la formation à la sécurité informatique, leur avis sur cette formation est comme suit :

Catherine : « *Et oui, comme j'ai dit, c'est vrai que ça change la donne pour la création des mots de passe donc c'est ça surtout. Ça sensibilise aussi dans le fond, surtout qu'on sait quand peut croiser toute sorte de chose quand on reste connectés sur internet mais ça nous sensibilise un petit peu plus en fait. Ils avaient parlé du dark web en particulier ça je ne connaissais pas du tout et après j'ai entendu parler d'internet gris ! Je me suis dit ah y a le gris aussi ! »*

Jennyfer : « *Oui, oui parce que j'avais par exemple le même mot de passe pour mon compte bancaire, ma boite mail et tout ça et du coup j'ai changé. J'ai changé, j'ai quand même des différents* », « *Pour le coup moi, avec une simple formation on nous a montré les dégâts qui pourraient nous faire ce type de problèmes, ça m'a fait prendre conscience qu'il faut faire attention et qu'il faut changer les mots de passe et ne pas avoir le même partout et pleins de choses d'autres* ».

Pierre : « *Joker sur cette question je devrais changer les codes d'accès. Plus souvent vous trouvez des codes d'accès un peu plus compliqués que ce que j'ai. J'avoue que maintenant, les sites vous obligent à mettre des codes de rallonge avec un signe d'être. C'est vrai que de ce côté-là non je n'ai pas fait trop d'efforts parce que je trouve que ça fait trop de codes à retenir. J'essaie de trouver les codes simples alors généralement je dis bien généralement au point de vue du travail il n'y a pas de code personnel qui pourrait être lié à ma famille ou autre ».*

Ces trois salariés ont le niveau de culture sécurité le plus **fort** (Niveau 3) et expriment l'intérêt de la formation reçue.

Pour les entreprises qui font de la sensibilisation sur le sujet de la sécurité des SI auprès de leurs équipes, nous trouvons l'entreprise **G** et l'entreprise **D** :

Le dirigeant de l'entreprise **D** exprime : *« En fait je les sensibilise quand moi-même j'ai des événements dont j'entends parler qui me resensibilisent et je les partage en fait »* (Sten).

Le directeur adjoint de l'entreprise **G** affirme : « *On essaie de sensibiliser les gens. On vient de mettre en place par exemple Vade sécure sur les boîtes mail un système, un logiciel qui analyse les mails entrants. Donc on a sensibilisé les gens, on est allés, c'est Orange qui faisait une réunion* » (André).

Pour ces deux entreprises qui sensibilisent leurs salariés au sujet de la sécurité, nous trouvons deux salariés interrogés (50% des interrogés) de l'entreprise **G** qui ont un niveau fort en culture sécurité, deux autres ont un niveau moyen et pour l'entreprise **D** le seul salarié interrogé (Sabine) à un niveau moyen de culture sécurité.

Nous ne trouvons ni formation, ni sensibilisation à la sécurité destinées aux utilisateurs des entreprises **B, C, E, F** et **H**. Les salariés de ces entreprises ont un niveau faible ou moyen en culture sécurité.

Niveau 1 (Faible) : 2 entreprises C, 2 entreprises H et 1 entreprise F
Niveau 2 (Moyen) : 1 entreprise C, 2 entreprises H, 2 entreprises E, 1 entreprise F
A l'exception de deux salariés de l'entreprise B (Maxime et Gaétan) qui ont un niveau fort en culture sécurité, ce qui peut être dû à d'autres facteurs.

Retour sur la littérature :

Ces constats nous permettent de mettre l'accent sur l'importance de la formation et de la sensibilisation ainsi que leurs influences positives sur la culture sécurité des utilisateurs. Ce qui est en cohérence avec les travaux de Djokovski et Al, 2007 pour les PME et Alnatheer, 2012 ; Da Veiga, 2015 pour les plus grandes organisations qui affirment qu'une formation à la sécurité pour les employés a une influence positive sur leur culture sécurité et une sensibilisation à la sécurité forme un pilier pour sa mise en place. (Hassan et Ismail, 2012 ; Da Veiga et Martins, 2015 ; Tolah et Al, 2017).

3. Orientation 3 : Le rôle de la direction

La direction de la PME joue un rôle important dans la création d'une culture sécurité SI. Pour évaluer la sensibilité du dirigeant à la sécurité, nous avons pris en considération son intérêt exprimé pour la sécurité, son rôle exercé pour impliquer les utilisateurs, les mesures de sécurité déjà prises au sein de l'entreprise et le budget consacré à la sécurité. Selon notre évaluation, les dirigeants les plus sensibles à la sécurité sont : le dirigeant de l'entreprise **B**, la direction de l'entreprise **A** et enfin, la direction de l'entreprise **G**.

Le dirigeant de l'entreprise **B** exprime : « *Mon rôle est absolument essentiel, c'est moi qui donne les objectifs et de par mon empreinte va créer la culture entreprise, t'as l'esprit du bout du collectif. Donc un rôle absolument essentiel ».*

« Oui clairement, oui ! Oui dans la mesure d'un risque, moi en tant que dirigeant je dois être garant de la performance de la structure et ça passe par le bon fonctionnement de l'ensemble des outils de l'entreprise et l'informatique est aujourd'hui un outil au cœur de notre quotidien donc il faut absolument que ça fonctionne. Donc effectivement, la maitrise des risques d'un dysfonctionnement, d'une attaque d'un hackeur est un paramètre à prendre en compte. Oui, le sujet m'intéresse clairement ». (Jean-Luc).

Les salariés de ces 3 entreprises ont les meilleurs niveaux de culture sécurité :
Niveau 3 (Fort) : 3*A, 2*G et 2*B
Niveau 2 (Moyen) : 2*G et 1*B

Pour les dirigeants les moins sensibles, nous trouvons le dirigeant de l'entreprise **F** qui est le moins sensible, le dirigeant de l'entreprise **H** et le dirigeant de l'entreprise **C**, avec le plus faible intérêt exprimé pour la sécurité, un faible rôle exercé pour impliquer les utilisateurs.

L'avis du directeur de l'entreprise **F** sur la sécurité : *« En fait c'est un sujet auquel je m'intéresse quand j'ai un problème. Lors de la mise en place du système informatique qui date d'il y a cinq ans. On est sur une version qui date de cinq ans, on réfléchit une bonne fois pour toutes dans les grandes lignes au principe de sécurité. Ensuite, on les met en place et six mois après, ils sont obsolètes. Donc on met les grands principes en place, quelques semaines après ils sont déjà obsolètes mais on passe à autre chose on n'a pas le temps. Et du coup, c'est quelque chose que je vérifie juste que mes sauvegardes se passent bien une fois par semaine. Mais ça s'arrête là. Rien de plus ! »* (Erwan)
En ce qui concerne le budget destiné à la sécurité : « *Mais si je doublais mon budget admettons, aujourd'hui je n'ai aucun intérêt puisque même en cas de soucis, ça ne me coûterait pas 15 000 euros quoi ! Donc si je rajoute 3000 ou 4000 euros par an supplémentaires pour la sécurité de toute façon au bout de 3 ou 4 ans globalement ça aura coûté plus cher au préventif qu'au correctif donc, je n'ai pas un grand intérêt ! Le jour où ça arrivera où il y aura quelque chose effectivement, il y aura quelque chose de plus conséquent à effectuer mais ça ne sera jamais complètement démesuré »* (Erwan)

L'avis du responsable informatique de l'entreprise **H** sur le budget sécurité : « *On essaie de ne pas augmenter le budget oui ! Après s'il y a un risque avéré on le fera mais on reste ! On n'est*

pas convaincus, quoi ! Aujourd'hui on a l'impression qu'on a des mesures et un budget qui est adapté à notre activité et aux risques qu'on concourt » (Bruno)

Si nous regardons le niveau de la culture sécurité des salariés appartenant à ces entreprises, nous trouvons :
Niveau 1 (Faible) : 2*H, 2*C, 1*F

Niveau 2 (Moyen) : 2*H, 1*C, 1*F

Les entreprises avec des dirigeants moyennement sensibles, comme ceux des entreprises **D** et **E** contiennent des salariés ayant un niveau moyen / 2 de culture sécurité : 2*E et 1*D

Ces résultats nous permettent alors de conclure que le dirigeant joue un rôle clé dans la sécurité de son entreprise ainsi que sur le niveau de culture de ses salariés. Donc, plus le dirigeant est sensible à la sécurité et investi, plus le niveau de culture sécurité de ses salariés augmente.

Retour sur la littérature :

Il était déjà démontré que les dirigeants de PME jouaient un rôle essentiel dans la protection des SI, au travers des actions qu'ils peuvent mettre en œuvre ou l'influence qu'ils ont sur leurs employés. (Dutta et McCrohan, 2002 ; Djokovski et al, 2007 ; Alnatheer, 2012 ; Barlette, 2017, Barlette et Jaouen, 2019).

Nos résultats sont en cohérence avec les travaux sur le TMS ou Top Management Support (Barlette, 2012 ; Boonstra, 2013), qui ont montré que le dirigeant avait une influence majeure sur : la validation de certains projets ; les budgets affectés à ceux-ci ; la communication auprès des employés ; les comportements des collaborateurs, surtout dans le cas des PME où le dirigeant joue un rôle central dans le choix et la mise en place des mesures et des contrôles liés à la sécurité des systèmes d'information.

Nous trouvons, dans la recherche de Barlette et Jaouen, (2019), une distinction des actions du dirigeant en actions de protection et actions de soutien à la sécurité des SI. Le directeur et les actions de la haute direction dans la sécurité des SI sont essentiels pour réduire les risques et garantir la conformité à la sécurité des SI des employés (de Guinea et al, 2005 ; Hu et al, 2012). De plus, dans les plus petites PME, il n'y a pas souvent de DSI, et même dans le plus grandes PME, les experts en SSI restent rares. Une autre délégation est possible : le dirigeant peut sous-traiter à des acteurs externes, telles que les sociétés de services informatiques. Cependant, dans tous les cas, la résolution des problèmes de la sécurité des SI ne peut pas être un emploi à temps plein pour les DSI ou les spécialistes informatiques externes (Barlette et Jaouen, 2019).

De plus, l'allocation de ressources est un aspect de soutien largement reconnu de la haute direction (Boonstra, 2013). Il correspond à l'allocation des fonds, à la validation des budgets, l'affectation de personnel à un projet informatique et à la création d'un contexte favorable qui facilite le flux de ressources destinées à l'informatique (Liu et al, 2015).

4. Orientation 4 : Relation culture-comportement

L'adoption d'une culture sécurité est favorable à créer un comportement lié à la sécurité . Si nous prenons la classification des salariés selon leurs niveaux de culture sécurité et nous la comparons avec la classification de ces mêmes salariés selon leurs niveaux de comportements liés à la sécurité, la classification selon les niveaux de culture et de comportements est présentée au sein du tableau suivant :

Niveau de culture		
Niveau 3 (Fort)	Niveau 2 (Moyen)	Niveau 1 (Faible)
Jennyfer (A), Pierre (A), Catherine (A), Mélissa (G), Pol-Lou (G), Maxime (B), Gaëtan (B),	Jonathan (C), Sabine (D), Marie (G), Brigitte (G), Julian (H), Sandrine (H) Maïwenn (F), Franck (E), Danielle (E), Marie-Laure (B)	Bénédicte (H), Christine (H), Marie (F), Fabien (C), Robin (C)
Niveau de comportements liés à la sécurité		
Niveau 3 (Fort)	Niveau 2 (Moyen)	Niveau 1 (Faible)
Jennyfer (A), Pierre (A), Catherine (A), Mélissa (G), Marie-Laure (B), Maxime (B), Gaëtan (B), Sabine (D),	Jonathan (C), Marie (G), Brigitte (G), Julian (H), Sandrine (H), Maïwenn (F), Danielle (E), Pol-Lou (G), Marie (F),	Bénédicte (H), Christine (H), Fabien (C), Robin (C), Franck (E)

Tableau 53 : Comparaison entre niveaux de CSSI et niveaux de comportements liés à la SSI des utilisateurs

17 utilisateurs sur 22 **(77%)** gardent le même niveau en culture sécurité qu'en comportements liés à la sécurité, ceux qui ont un niveau fort en culture sécurité (propriété, conscience et conformité) restent sur le niveau 3 (fort) dans la classification des comportements liés à la sécurité (politique liée aux mots de passe, sauvegardes), ceux qui ont un niveau moyen en culture gardent un niveau moyen en comportements et enfin, ceux qui sont classés au niveau faible de culture sécurité ont aussi un niveau faible de comportements liés à la sécurité.

A l'exception de **2** utilisateurs où leurs niveaux de comportements liés à la sécurité se dégradent d'un niveau par rapport à leur culture sécurité :

Pol-Lou avec un niveau **fort** en culture et un niveau **moyen** en comportements liés à la sécurité

Franck avec un niveau **moyen** en culture et un **faible** niveau de comportements.

Et **3** autres utilisateurs dont leurs niveaux de comportement liés à la sécurité augmentent d'un niveau par rapport à leur culture sécurité :
Marie-Laure et **Sabine** niveau **moyen** en culture et niveau **fort** en comportements

Marie de l'entreprise **F** d'un niveau **faible** de culture à un niveau **moyen** de comportements liés à la sécurité.

Ces changements de niveau sont peut-être dus à d'autres facteurs. Nous avons par exemple l'explication de Franck qui exprime une difficulté en ce qui concerne la complexité des mots de passe choisis et qu'il préfère mettre des mots de passe faciles à retenir, donc qui réfèrent à des éléments personnels comme date, lieu de naissance, etc. *« Parfois il y a des mots de passe sécurisés où on met des majuscules mais la plupart du temps, je mets des trucs faciles à retenir »* (Franck).

Un autre exemple de Marie-Laure qui a un niveau de culture sécurité moyen et exprime son avis sur le choix des mots de passe comme suit : « *Non, ça j'ai essayé de ne pas mettre des données personnelles dedans parce que je sais que les hackeurs pourront retrouver des dates, oui par précaution je n'ai pas mis oui !* » (Marie-Laure).

Au vu de ces résultats significatifs 77% des interrogés qui ont le même niveau en culture sécurité que pour leurs comportements liés à la sécurité, donc plus le niveau de culture sécurité augmente plus les comportements en matière de sécurité s'améliorent.

Retour sur la littérature :

Ce résultat est en cohérence avec l'étude de Parsons et al (2015), qui montre que la culture SSI exerce une influence notable sur l'attitude des employés à l'égard de la politique et des procédures de sécurité. L'étude de Flores et al (2016) est la seule étude à avoir examiné une relation plus complète entre la CSSI et le comportement en matière de sécurité. Bien qu'ils ne se soient pas concentrés uniquement sur l'effet du concept de la culture SSI sur le comportement en matière de sécurité, leurs conclusions ont fourni des résultats plus complets sur la relation entre la culture sécurité et le comportement des employés en matière de sécurité par rapport à d'autres études. Plus précisément, ils ont constaté que la culture sécurité avait un effet significatif sur l'attitude et la croyance normative en matière de résistance à l'ingénierie sociale.

Une autre étude plus récente de Connolly et Al (2017) montre l'influence de la culture organisationnelle, des contre-mesures et des procédures de sécurité sur les comportements sécuritaires des employés. Leur étude montre que l'effet dissuasif des contre-mesures

procédurales de sécurité augmente la sensibilisation à la SSI. Cette prise de conscience, à son tour, tend à empêcher les actions malveillantes des employés et encourage les comportements sécuritaires. Nos résultats s'ajoutent à ces études afin de montrer l'importance d'une culture sécurité qui résulte de plusieurs facteurs, dont la sensibilité du dirigeant à la sécurité, la formation et la sensibilisation etc., dans l'influence sur les comportements liés à la sécurité et plus particulièrement, dans le cadre des PME.

5. Émergence d'autres facteurs

5.1 Différence entre générations (âge de l'utilisateur)

Lors des interviews, nous constatons que **cinq** salariés évoquent la différence entre les générations : « *Moi, je suis concerné et préoccupé par les problèmes de sécurité, mais comme je vous ai dit, je n'ai pas cette culture informatique, et avec la couleur de mes cheveux vous vous dites que je suis en fin de carrière aussi ! (Rigole) Donc, j'ai vu l'informatique arriver, pour moi on n'a pas cette connaissance que les jeunes d'aujourd'hui ont déjà je pense, car je ne sais pas s'ils sont plus sensibles que nous à la sécurité mais ils comprennent davantage les systèmes parce qu'ils sont nés avec l'informatique* » (Brigitte, **61 ans**)

Elle rajoute : « *Mais je pense que je n'ai pas sûrement la même vision des choses que quelqu'un qui est très (très) jeune dans l'entreprise. Vous avez vu Pol-Lou tout à l'heure, je pense que lui il est beaucoup plus au fait sans le tas de certaines choses et de part de sa fonction aussi. Je pense qu'il y a un tas de choses qui font que la sécurité est prise en compte je pense, différemment, en fonction des personnes, de l'âge, de la fonction... Il y a pleins de facteurs* ».

« *Mais, j'ai l'impression par rapport aux autres générations, comme Jennyfer qui a participé aussi à la formation, je pense que je connais moins que cette génération-là. A l'âge de mes enfants en fait, j'ai l'impression que j'apprends aussi avec mes enfants sur ces choses-là parfois. Mais je me trouve un peu psychorigide avec ma sécurité. Donc, je connais un petit peu* (Rigole). » (Catherine, **52 ans**).

« *Non ! Parce que je suis d'une génération où on ne se préoccupait pas de la sécurité informatique, je pense que mes enfants ou mes petits enfants seront plus sensibilisés à ça c'est sûr !* » (Danielle, **55 ans**).

Ces trois utilisatrices expliquent qu'elles connaissent moins de choses liées à l'informatique et à la sécurité par rapport à leurs collègues plus jeunes, l'exemple de Pol-Lou (**23 ans**) et Jennyfer (**33 ans**), ou par rapport à leurs enfants.

Dans un autre côté, les plus jeunes salariés sont Maxime et Pol-Lou, et expriment à leur tour leur avis de la manière suivante : « *Comme j'ai dit, je suis sensible à ce genre de problème. J'utilise beaucoup l'ordinateur comme tous les gens de mon âge en fait, donc c'est un problème où je suis assez sensible* » (Maxime, **22 ans**).

« *Je pense que vous allez voir Brigitte tout à l'heure elle ne va pas forcément comprendre ! Je ne pense pas et puis surtout que les générations sont plus près certains de la fin qu'ils n'ont pas grandi avec les smartphones des choses comme ça où tout ça, je pense que c'est assez difficile pour eux donc je conçois que l'entreprise au niveau information là-dessus on n'est pas assez encore informés quoi !* » (Pol-Lou, **23 ans**)

Ces deux jeunes salariés pensent qu'ils sont plus sensibles à la sécurité et plus à l'aise avec tout ce qui est nouvelles technologies par rapport aux personnes les plus âgées.

Si nous revenons à la typologie des salariés et que nous regardons l'âge des utilisateurs qui ont le plus **haut** niveau de culture sécurité par rapport aux autres ;
Jennyfer : 33 ans, Pierre : 39 ans, Catherine : 52 ans, Mélissa : 39 ans, Maxime : 22 ans, Gaétan : 51 ans, Pol-Lou : 23 ans. Nous remarquons que les salariés les moins âgés (22 ans et 23 ans) sont situés dans cette catégorie à l'exception de Catherine et Gaétan qui ont un âge supérieur à 50 ans. Pour Catherine (52 ans) de l'entreprise **A** obtient un score moins élevé que ses collègues Jennyfer (33 ans) et Pierre (39 ans), malgré le fait qu'elle a reçu la même formation à la sécurité et appartiennent à la même entreprise qui a un bon niveau en termes de mesures de sécurité mises en place.

Pour les utilisateurs qui ont le plus **faible** niveau de culture sécurité, nous avons :
Bénédicte : 55 ans, Christine : 45 ans, Marie : 24 ans, Fabien : 37 ans et Robin : 33 ans, pour Marie la plus jeune entre eux, nous remarquons que son niveau de comportements liés à la sécurité est passé à un niveau **moyen,** ce qui peut être modéré par son jeune âge où elle est plus à l'aise avec tout ce qui est lié à l'informatique.

Prenons maintenant l'exemple de l'utilisatrice Maïwenn (28 ans) ; malgré le fait qu'elle appartienne à l'entreprise **F** avec le plus **faible** niveau de sécurité, elle est classée dans un niveau **moyen** de culture sécurité ainsi que de comportements liés à la sécurité.

Nous avons aussi dans l'entreprise **G** qui a un niveau de sécurité fort, deux salariés qui ont un niveau **fort** de culture sécurité Mélissa (39 ans) et Pol-Lou (23 ans) ainsi que deux salariés avec un niveau **inférieur** aux deux premiers, à savoir Brigitte (61 ans) et Marie (51 ans).

A partir de ces constats, nous pouvons dire que l'âge de l'utilisateur peut jouer un rôle modérateur sur la relation entre sa culture sécurité et ses comportements effectifs liés à la sécurité, sur la relation entre la formation (sensibilisation) et la culture sécurité et enfin, entre les mesures de sécurité mises en place par la direction et la culture sécurité.

Retour sur la littérature :

Selon une recherche réalisée par Lancelot Miltgen et Peyrat Guillard (2014) concernant l'influence culturelle et générationnelle sur les préoccupations de confidentialité, en ce qui concerne l'âge, elles ont constaté que les jeunes se sentent plus positifs, plus responsables et plus confiants dans leurs capacités à prévenir une éventuelle utilisation abusive des données, et ils font plus confiance à l'efficacité de la protection juridique que les adultes. Inversement à ces résultats, d'autres études montrent que les personnes âgées de 18 à 25 ans étaient plus vulnérables au phishing que les groupes plus âgés (Sheng et al 2010). Et Pattinson et al, (2015), ont trouvé une relation positive significative entre l'âge et le comportement dans le domaine de la sécurité du SI, indiquant que les personnes âgées peuvent avoir un meilleur comportement.

Nos résultats sont plus en harmonie avec ceux de Miltgen et Guillard (2014), dans le sens où plus la personne est jeune, plus sa culture sécurité est susceptible d'être plus forte et son comportement lié à la sécurité peut être meilleur. Cela peut être expliqué par la familiarité des jeunes (Entre 18 et 40 ans) avec les outils informatiques, les réseaux sociaux, les nouvelles technologies, ce qui peut favoriser une plus grande aisance dans le traitement des informations à travers ces outils et ces technologies, ce qui peut expliquer le moins de rigidité en termes de compréhension et d'application des mesures de sécurité.

5.2 Le poste occupé par l'utilisateur

Deux utilisatrices évoquent la sensibilité de leurs postes à la sécurité et la confidentialité des données traitées :

« *Moi mon rôle, je pense que je dois faire beaucoup plus attention que certains salariés de l'entreprise, par exemple les postes dans l'atelier, moi je suis susceptible d'utiliser les ordinateurs, et j'ai beaucoup d'informations qui sont confidentielles, donc j'ai un poste où je*

dois faire très attention et après, j'essaie aussi de faire comprendre aux autres que certaines informations, je ne peux pas les transmettre et qu'il faut faire attention dans leurs boites mails, donc voilà. » (Jennyfer, **Assistante de direction-RH**)

« *Oui ! Surtout où on est dans notre service ressources humaines, c'est vrai qu'on gère beaucoup les informations personnelles des salariés. Donc je pense qu'on a quand même intérêt à faire attention à ce qu'on fait parce que ça ne nous concerne pas et que ça concerne aussi tous les salariés de l'entreprise, donc je pense que on nous demande aussi d'être vigilants s'ils voulaient encore plus maintenant avec les nouvelles lois, le RGPD tout ce qui va avec. Je pense qu'on est responsables. En tout cas surtout dans mon service je trouve après que nous on doit faire très attention !* » (Mélissa, **Responsable RH-Paye**)

Ces deux utilisatrices ont un niveau **fort** de culture sécurité ainsi que de comportements liés à la sécurité, où elles déclarent qu'elles font beaucoup plus attention par rapport aux autres salariés de l'entreprise.

Prenons aussi les témoignages suivants :

« *Pourquoi pas faire des réunions avec le service informatique pour qu'il nous explique que ça il faut faire ci, s'il faut faire ça et faire attention et surtout pour les gars de l'atelier qu'ils font peut-être moins attention. Je ne sais pas après peut être moins attention que nous parce qu'ils utilisent moins l'ordinateur et c'est justement là qu'il peut avoir des failles là-dedans* » (Jennyfer, **Assistante de direction-RH**)

« *Une formation c'est clair ! Mais après est-ce que c'est utile, je ne sais pas ! Parce que, si quelqu'un qui travaille ici, il sera intéressé par ça ?! Vous voyez ! Ça dépend des postes, peut-être un peu plus dans le bureau* ». (Marie, **Assistante direction polyvalente**)

« *Je pense qu'il y a un tas de choses qui font que la sécurité est prise en compte je pense différemment, en fonction des personnes, de l'âge, de la fonction, il y a pleins de facteurs* ». (Brigitte, **Employé d'accueil**).

Ces trois utilisatrices évoquent l'importance du poste dans la prise en compte de la sécurité des SI ainsi que pour la formation liée à la sécurité.

Si nous prenons les utilisateurs qui ont le plus haut niveau en comportements liés à la sécurité :

Jennyfer : **Assistante de direction-RH,**
Pierre : **Comptable-Fournissuers**,
Catherine : **Comptable-Clients**,
Mélissa : **Responsable RH-Paye,**
Maxime : **Assistant qualité**
Gaétan : **Responsable service conditionnement**
Marie-Laure : **Assistante administrative**
Sabine : **Secrétaire comptable**

Pour les utilisateurs qui ont le plus **faible niveau** en comportements liés à la sécurité :

Bénédicte : **Comptable**
Christine : **Service qualité**
Fabien : **Chargé d'affaire**
Robin : **Concepteur en bureau d'étude**
Franck : **Chiffreur, métreur, dessinateur**

Nous constatons que pour les utilisateurs qui ont plus de comportements liés à la sécurité par rapport aux autres occupent des postes sensibles à la confidentialité des données (75%) comme les postes d'RH, d'assistance à la direction ou de comptabilité.
Pour les utilisateurs qui ont moins de comportements liés à la sécurité par rapport aux autres utilisateurs, ces derniers occupent des postes les moins sensibles à la confidentialité des données (80% d'entre eux) comme par exemple les postes les plus techniques : les poste de chargés d'affaires ou les postes liés à la conception.

Ces constats nous permettent de mettre la lumière sur le rôle modérateur du poste occupé par l'utilisateur dans la relation entre la culture sécurité et le comportement effectif lié à la sécurité, où le type de poste occupé peut renforcer les comportements liés à la sécurité s'il est lié à des données sensibles ou confidentielles.

Retour sur la littérature :

Si nous revenons à la littérature, il a été constaté que les postes (rangs) des employés ont un impact positif sur la conformité à la politique de sécurité des SI (Guo & Yuan, 2012).

Selon Barlette (2005), parmi les facteurs de motivation aux comportements liés à la sécurité, nous trouvons le poste ou la fonction occupée par le salarié, tels que les postes liés à la R.H (Ressources Humaines), la comptabilité etc. qui sont des postes plus sensibles à la sécurité des données, où le salarié doit avoir un minimum de confidentialité.

A notre connaissance, nous n'avons pas identifié d'autres études qui ont testé l'effet du poste occupé par l'utilisateur sur sa culture sécurité des SI. Ce qui peut être exploré et testé au travers des futures études quantitatives.

Synthèse de la section 1

Tout au long de cette section, nous avons examiné les orientations de recherche établies au niveau du deuxième chapitre. Nous avons pu à travers notre étude terrain, confirmer nos quatre orientations de recherche, en confrontant nos résultats avec ceux des recherches antérieures. De nouveaux facteurs ont émergé du terrain, à savoir l'âge et le poste de l'utilisateur, où nous allons les intégrer au sein de notre modèle conceptuel qui sera présenté dans la section suivante (section 2).

Section 2 : Retour sur le modèle conceptuel

Suite à l'étude qualitative réalisée et après l'examen de nos quatre orientations de recherche et la discussion de nos résultats avec la littérature, nous allons dans cette section réviser notre modèle initial en rajoutant les éléments qui ont émergé de notre étude qualitative. Ensuite, nous allons discuter de la qualité de cette étude qualitative réalisée.

1. Révision du modèle conceptuel initial

Selon nos résultats précédents, nous gardons les facteurs initialement identifiés à partir de la littérature, à savoir :

-Les facteurs qui constituent la culture sécurité : propriété de sécurité, conscience et conformité.
-Les facteurs qui influencent la culture sécurité : contexte réglementaire et légal, prestataire de services informatiques, secteur d'activité, gestion des risques, formation et sensibilisation, sensibilité du dirigeant.

Néanmoins, nous rajoutons en premier lieu l'influence des facteurs exogènes (contexte règlementaire et légal, prestataire de services informatiques, secteur d'activité) sur la sensibilité du dirigeant, puisque nous avons relevé que s'il existe un accompagnement de la part du gouvernement, l'existence des lois comme l'RGPD, le dirigeant de la PME va se sentir plus orienté dans la gestion de la sécurité de son entreprise. Et s'il existe une relation de confiance entre le client (la PME) et son prestataire informatique et que ce dernier joue un rôle de conseil et de support technique. Cela peut soutenir la direction de la PME dans la gestion de la sécurité de son SI. En ce qui concerne le secteur d'activité, nous avons pu relever d'après nos résultats, que les secteurs comme celui du commerce par exemple dont les personnes de la direction interrogées, pensent qu'ils ne sont pas sur un domaine très stratégique et que les données ainsi que les informations traitées au sein de leurs entreprises ne sont pas d'ordre confidentiel, ce qui laisse les mesures de sécurité non prioritaires et qu'ils n'ont pas besoin d'un niveau de sécurité élevé. Donc, nous pouvons dire que si le secteur d'activité de la PME est lié à des informations confidentielles ou sensibles tels que les secteurs liés à l'aéronautique, le nucléaire, la télécommunication etc. Le dirigeant peut être plus sensible à la sécurité de son SI et ainsi, susceptible de mettre en place des mesures de sécurité afin de protéger au mieux les données traitées par son entreprise.

En deuxième lieu, nous rajoutons l'influence de la direction sur la mise en place des actions de gestion des risques, de formations et de sensibilisations (qui représentent les facteurs endogènes), car une fois que la sensibilité du dirigeant à la sécurité augmente, les mesures de sécurité telles que la gestion des risques et les actions de formation et sensibilisation vont être mises en place. Finalement, nous avons additionné l'âge et le poste de l'utilisateur comme facteurs modérateurs entre la culture sécurité et le comportement lié à la sécurité. Nous allons présenter le modèle issu des résultats de l'étude qualitative dans la figure suivante :

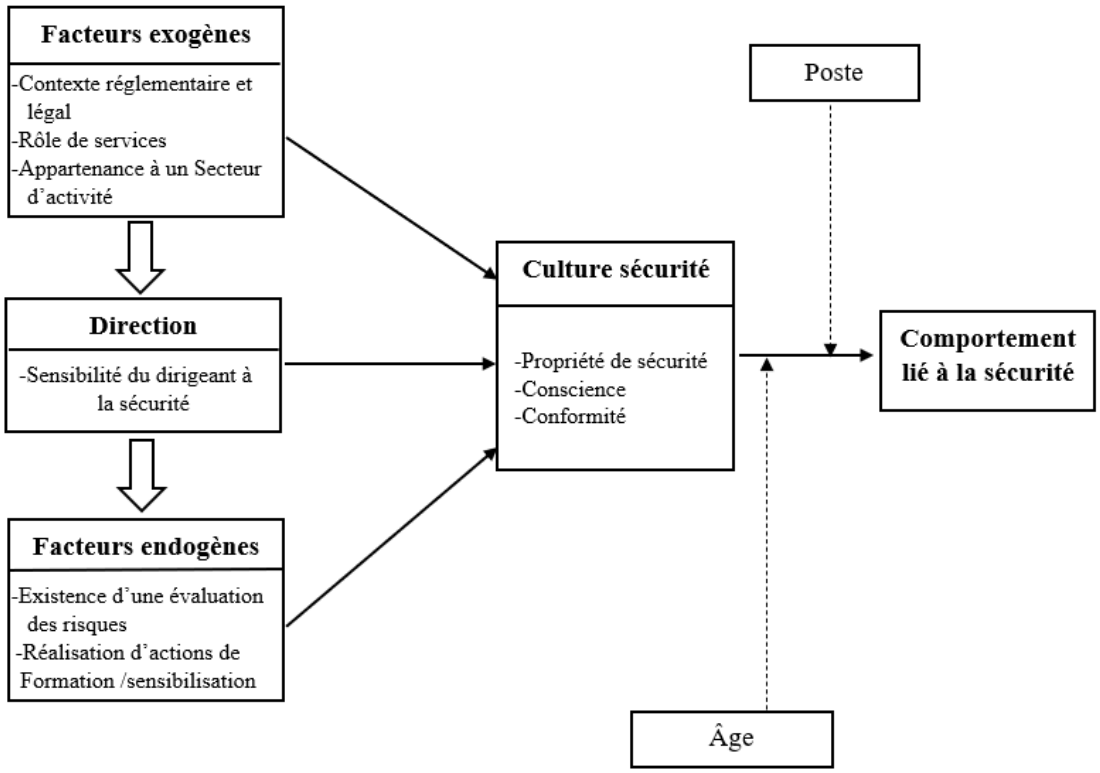


Figure 37 : Modèle de recherche revisité

Maintenant que nous disposons des facteurs principaux, une étude quantitative à grande échelle des salariés pourrait permettre d'affiner les facteurs qui influencent et qui composent la culture sécurité, mais aussi de tester les facteurs modérateurs dans la relation entre la culture sécurité et les comportements liés à la sécurité. Notre étude était exploratoire, il ne nous était pas possible d'explorer toutes les pistes qui se posent dans ce domaine passionnant, mais nous allons ouvrir de nombreuses pistes de recherche futures au niveau de notre conclusion générale de ce travail.

2. Qualité de l'étude qualitative

Pour conclure cette étude qualitative, il convient de s'interroger sur la qualité des résultats obtenus. Pour cela, nous appliquerons la méthode de Miles et Huberman (2003), qui consiste à se poser des questions relatives à des critères de qualité.

Miles et Huberman (2003), posent une quarantaine de questions, qui doivent cependant être considérées comme des pistes de réflexion et non des règles strictes. Pour avoir davantage de clarté, nous présentons une synthèse de ces critères de qualité dans le tableau suivant :

Critère de qualité	Elément de réponse à propos notre recherche
Objectivité / Confirmabilité	
Traçabilité du processus de recherche	Nous avons détaillé les diverses étapes de la recherche dans le début du chapitre. Toutes les données ont été conservées et classées selon leur nature, plus ou moins brute. Nous avons distingué : enregistrements audio, retranscriptions, fiches de synthèse, fichiers de codage.
Limitation des biais d'influence et d'interprétation	Ce sont les fichiers de retranscription brute qui ont servi de base au codage sur Nvivo, comme si nous repartions de zéro, de manière à éviter les conclusions prématurées. Lors de la phase de terrain, nous avons essayé de faire - le plus possible - abstraction des théories, qui auraient pu influencer les réponses des interviewés
Fiabilité, sérieux, audibilité	
Cohérence et stabilité du processus de recherche	En cohérence avec notre positionnement épistémologique interprétativiste, les thèmes du guide d'entretien correspondent à des variables du modèle, déduites de la littérature. De plus, sur le terrain, nous avons respecté les profils de répondants définis initialement. Ainsi, nous avons maintenu une certaine cohérence entre la théorie, les questions de recherche et la mise en œuvre de l'étude qualitative.
Limitation des biais relatifs aux répondants	Nous avons vérifié que le répondant ne soit pas informé à l'avance des questions qui allaient lui être posées (aucun guide d'entretien n'a été envoyé à l'avance). Les répondants nous ont semblé tous sincères et spontanés, lors des entretiens.
Limitation des biais relatifs au codage	Avant de procéder à la phase d'analyse, nous avons repris un à un les codes afin d'en examiner le contenu et de détecter les erreurs d'affectation de verbatim dues à des difficultés de classification ou de manipulation du logiciel. De plus, un double codage a été effectué par un autre chercheur (taux d'accord initial = 80% ; après discussion =100%).

Validité	
Validité interne, crédibilité, authenticité	Nous avons essayé de retranscrire au mieux la diversité des expériences et des opinions de nos répondants. Après la transcription des entretiens, le contenu a été envoyé au répondant concerné pour vérifier l'intégralité de son discours et si des modifications ou des fautes d'inattention ont été commises. Ensuite et après l'approbation du répondant, nous avons pu utiliser le contenu de l'entretien dans l'analyse. Après l'aboutissement de notre modèle conceptuel à partir des études de cas, nous avons confronter ce modèle et les principaux résultats par un retour vers les dirigeants des PME à travers des échanges téléphoniques afin de vérifier le degré de validité de nos résultats.
Validité externe, transférabilité, intégration	Les caractéristiques de l'échantillon original ont été suffisamment décrites pour permettre des comparaisons avec d'autres échantillons. Ainsi, l'échantillonnage paraît assez diversifié pour encourager une généralisation à l'ensemble des utilisateurs du SI dans les PME.
Utilisation, application, prescription	
Portée de la recherche	Les résultats peuvent permettre la création d'une échelle de mesure de la culture sécurité des utilisateurs et guider des hypothèses de recherche. Les illustrations par les verbatim permettent également l'accessibilité et la compréhension des résultats par le plus grand nombre. Ainsi, les dirigeants des PME et les responsables des SI sont susceptibles de rapprocher facilement les propos des interviewés de ceux de leurs salariés.
Considérations éthiques	Nous avons sollicité systématiquement l'accord des individus, avant tout enregistrement. Aussi, nous avons gardé l'anonymat des entreprises étudiées ainsi que des répondants vu la sensibilité du sujet étudié (La sécurité des SI) et suite à leurs demandes.

Tableau 54 : Evaluation de la qualité de la recherche qualitative adaptée de (Miles et Huberman, 2003)

3. Réponse à la question de recherche

Si nous revenons à notre question de recherche initiale : « **Comment insuffler une culture sécurité des systèmes d'information en PME** », pour répondre à cette question et en se basant sur nos résultats de recherche précédemment discutés, nous proposons un processus comprenant un ensemble d'actions à mettre en place sur chaque orientations de recherche, le processus sera décrit ci-après :

3.1 Actions liées aux facteurs exogènes

Une PME peut se conformer à l'RGPD en mettant en place quatre étapes clés :

Etape 1 : identification des activités principales qui nécessitent la collecte et le traitement de données (exemples : gestion de la paie, gestion des badges et des accès, gestion des clients), en s'appuyant sur le modèle de registre proposé par la CNIL sur son site internet[31], et qui comprend des dispositions pour les organismes de moins de 250 salariés.

Etape 2 : trier les données, pour chaque fiche de registre créée, il faut vérifier, que les données traitées soient nécessaires aux activités de l'entreprise, cependant il faut avoir le droit de traiter des données que si elles sont dites sensibles, seules les personnes habilitées ont accès aux données dont elles ont besoin qui ne seront conserver au-delà de ce qui est nécessaire.

Etape 3 : respecter les droits des personnes en les informant à chaque fois qu'il y'a une collecte des données personnelles, le support utilisé (formulaire, questionnaire, etc.) doit comporter des mentions d'information.

Etape 4 : sécuriser les données de son entreprise, et garantir le patrimoine de données en minimisant les risques de pertes de données ou de piratage. Différentes actions doivent être mises en place afin de minimiser les risques de pertes de données, telles que les mises à jour des antivirus et logiciels, changement régulier des mots de passe et utilisation de mots de passe complexes, ou chiffrement des données dans certaines situations.

Parmi les avantages de la mise en conformité aux règles de protection des données, nous pouvons citer : le renforcement de la confiance de toute personne qui confie ses données

[31] https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement

personnelles à l'entreprise, l'amélioration de l'efficacité commerciale et l'amélioration de la sécurité des données de l'entreprise.

Nous trouvons aussi, des actions de formations et de sensibilisation à la sécurité des SI et à la cyber sécurité mise en place par la CCI (Chambre de commerce et de l'industrie), citant en exemple : le ''Colloque cyber sécurité : la normalisation au cœur du dispositif'' sur les bonnes pratiques et les besoins de demain pour protéger les données et l'ensemble des systèmes d'information et de communication des entreprises, ainsi que des rencontres avec des professionnels de la sécurité pour orienter et sensibiliser les dirigeants et les responsables des PME à la sécurité des données et des systèmes d'information. Nous estimons, que la participation des dirigeants et des responsables de PME, notamment des DSI et des responsables informatiques, à ces évènements et aux rencontres de sensibilisation est très importante dans le sens où elle peut encourager les prises de décisions concernant la mise en place des actions de sécurité et surtout la prise de conscience des risques et des menaces qui peuvent perturber le fonctionnement des entreprises.

De plus, l'ANSSI et le gouvernement, ont mis en place sur la plateforme *cybermalveillance.gouv.fr*, des bons réflexes et des conseils nécessaires pour la formation des salariés à la sécurité des SI. De telles conseils, peuvent être consultables par les responsables des PME et recommandés aux salariés.

Il sera très intéressant de bien choisir son prestataire informatique, avec lequel une relation de confiance peut être établie, un bon prestataire informatique peut jouer un rôle de conseiller sur le niveau de sécurité nécessaire pour une PME, sur les mesures de sécurité à mettre en place pour sécuriser le matériel informatique (hardware) et les logiciels (software) fournis par le prestataire. Des tests réguliers de sécurité du système d'information de la PME, peuvent être réalisés par le prestataire pour s'assurer que le niveau de sécurité au sein de la PME est acceptable, avec des propositions de solutions et de plans d'actions en cas de problèmes.

3.2 Actions liées à la direction de la PME

Afin d'augmenter la sensibilité des dirigeants de la PME à la sécurité du SI, chaque dirigeant doit avoir un minimum d'informations sur comment sécuriser son SI, en participant par exemple à des sessions de formation et de sensibilisation destinées aux PME et proposées par l'Etat, notamment par la CCI ou l'ANSSI , afin d'être à jour sur les mesures de sécurité nécessaires à

mettre en œuvre et d'être sensibilisé aux différents risques qui peuvent influencer le SI et en conséquence l'activité générale de la PME.

Chaque dirigeant d'une PME traitant des données sensibles, doit réfléchir à la mise en place des actions de conformité à l'RGPD en suivant les quatre étapes mentionnées au niveau des actions liées aux facteurs exogènes.

Nous remarquons ici la grande influence qui peuvent jouer les actions liées aux facteurs exogènes sur le degré de sensibilité du dirigeant à la sécurité de son SI et à la prise de conscience des avantages de la mise en place des actions et des mesures de sécurité.

Chaque dirigeant de PME doit consacrer un budget destiné à la sécurité qui doit être dépendant du budget destiné à l'informatique. Ce budget doit varier selon les besoins de sécurité nécessaires à chaque PME, et qui va être destiné à mettre en œuvres des actions liées aux facteurs endogènes développées au niveau du titre suivant (3.3).

3.3 Actions liées aux facteurs endogènes

Chaque PME, peut identifier, évaluer et gérer les risques liés à son système d'information en mobilisant des méthodes de gestion des risques, nous allons citer comme exemple des méthodes que nous estimons les plus adaptées à mettre en place dans une PME :

L'utilisation d'une AMDEC (Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité) pour identifier les risques qui peuvent impacter le SI de la PME ensuite d'évaluer le niveau de criticité de ces risques et enfin de proposer des actions préventives afin d'éviter ou minimiser les risques et des actions correctives pour corriger ou réduire les impacts des risques. Une telle méthode peut être mise en place soit par le DSI ou le responsable informatique ou par le dirigeant lui-même.

Une matrice des risques peut également être utilisée pour évaluer les risques liés aux SI de la PME, en indiquant si un risque est acceptable, acceptable sous conditions ou inacceptable et cela est déterminé par une évaluation à deux dimension : probabilité et impact du risque. Dans le cas où le risque est inacceptable il faut mettre en place des actions pour faire face à ce risque.

La PME peut aussi transférer les risques (les externaliser) en inscrivant une assurance contre les fraudes et vols de données (escroquerie, atteinte aux systèmes d'information etc.), cette dernière peut couvrir la PME en cas de pertes.

Plusieurs assurances proposent des offres adaptées aux PME, prenons en exemple l'offre d'une assurance dont nous gardons l'anonymat : une solution adaptée aux PME et TPE pour faire face aux nouvelles menaces informatiques, la prise en charge des frais en cas de cyber attaque, d'erreur humaine, de vol de données ou de cyber fraude, à partir de 200 € TTC par an, ce que nous jugeons abordable pour une PME avec des moyens modestes.

Afin de mieux gérer les risques, un plan de reprise d'activité (PRA) et/ou un plan de continuité d'activité (PCA) peuvent être mise en place par la PME, nous allons définir en premier lieu les deux plans le PRA et le PCA ensuite comment les mettre en place.

Un PRA est une procédure qui permet d'assurer la reprise des activités, en mode dégradé ou à plein régime, d'une entreprise en cas de sinistre (inondation, coupure électrique, incendie, destruction de données vitales…). C'est un document qui répertorie les démarches à entreprendre pour reconstruire son système informatique en cas de crise importante et la remise en route des applications nécessaires aux activités d'une entreprise.

Un PCA est une procédure qui permet d'assurer la continuité des activités d'une entreprise, sans perte de données et qui offrira un accès au SI sans rupture d'exploitation.

Pour mettre en place un PRA et/ou un PCA, tout d'abord, il faut identifier les ressources critiques que l'entreprise souhaite protéger car elles sont indispensables à son bon fonctionnement. Ensuite il faut identifier le lieu où l'entreprise souhaite mettre en place le plan de reprise ou de continuité d'activité avec 2 solutions : soit sur un des sites de l'entreprise soit sur un site externe de type data center.

Une démarche de PCA/PRA comporte généralement les étapes suivantes :

- Définition des enjeux, des exigences et des besoins en matière de disponibilité des données et de processus critiques
- Classification des informations et des actifs de l'entreprise
- Analyse des risques du système d'information
- Définition du PCA ou du PRA
- Définition des processus de gouvernance et de gestion de la crise
- Accompagnement lors des phases de tests

Dans le cadre d'une PME, cette dernière peut externaliser la mise en place d'un PCA et/ou PRA en faisant appel à un prestataire spécialisé, car une PME n'a pas toujours les compétences

nécessaires, pour mettre en place une telle démarche. Ensuite, la PME peut négocier avec son prestataire, ses besoins en termes de niveau de protection souhaité qui dépend du domaine d'activité et du niveau de dépendance envers son SI. Des offres sont adaptées aux caractéristiques des PME, avec la prise en compte des ressources limitées et la proposition des démarches compréhensibles et faciles à mettre en place.

Le choix entre PRA et PCA, peut se faire de la manière suivante, si la PME peut se permettre des pannes des systèmes d'informations de courtes durées, la mise en place d'un PRA est envisageable puisqu'il vise à instaurer une procédure destinée à reprendre l'activité le plus vite possible. Un PCA est à privilégier si la PME ne peut aucunement se permettre de panne, même de courte durée.

Des actions de formation et de sensibilisation à la sécurité des SI peuvent être mise en place aux sein de la PME, destinées aux dirigeants, responsables et salariés qui sont tous utilisateurs du SI de l'entreprise. Ces actions doivent être adaptées au contexte de la PME, avec une démarche simple et peu coûteuse, nous pouvons citez à titre d'exemple les actions suivantes :

- Des MOOC dédiés à la sécurité des systèmes d'information à courtes durées et gratuits, tels que, le MOOC[32] Sécurité Numérique proposé par l'ANSSI[33], qui est une formation gratuite, élaborée par des experts en sécurité informatique et facilement diffusable au sein d'une entreprise, le suivit intégral de cette formation permet de bénéficier d'une certification.
- Former, un seul responsable ou salarié à la sécurité des SI qui peut ensuite former à son tour les autres utilisateurs au sein de la PME.
- Choisir des formations simples, courtes et ludiques pour attirer l'attention des utilisateurs et garantir l'efficacité de ces formations et éviter les formations trop techniques pour ne pas décourager les participants qui n'ont pas des connaissances approfondies dans le domaine informatique.
- Faire des rappels périodiques des bonnes pratiques de sécurité : envoie des mails de rappel, des questionnaires destinés aux utilisateurs pour évaluer leurs niveaux de sécurité, des tests d'intrusion fictifs pour vérifier si les utilisateurs gardent toujours les bons réflexes face aux menaces etc.

[32] Massive Open Online Course
[33] Agence Nationale de la Sécurité des Systèmes d'Information

Des actions techniques liées à la partie technique du système d'information : logiciels, matériels, serveurs, infrastructures etc. peuvent être mise en place par les PME pour sécuriser leurs SI, nous allons citer les actions les plus indispensables :

- **Authentifier les utilisateurs :** assurer qu'un utilisateur accède uniquement aux données dont il a besoin
- **Tracer les accès et gérer les incidents : t**racer les accès et prévoir des procédures pour gérer les incidents afin de pouvoir réagir en cas de violation de données
- **Sécuriser les postes de travail :** mettre en place des pare-feu, antivirus, mise à jour régulière des logiciels et antivirus, limiter la connexion de supports mobiles (clés USB, disques durs externes, etc.)
- **Protéger le réseau informatique interne :** limiter les accès Internet, **g**érer les réseaux Wi-Fi**,** utiliser un chiffrement à l'état de l'art (WPA2 ou WPA2-PSK avec un mot de passe complexe) et les réseaux ouverts aux invités doivent être séparés du réseau interne.
- **Sécuriser les serveurs et les sites web :** renforcer les mesures de sécurité appliquées aux serveurs**, s**'assurer que les bonnes pratiques minimales sont appliquées aux sites web.
- **Chiffrer, garantir l'intégrité ou signer :** les signatures numériques, le chiffrement (Cryptographie), utilisation d'un algorithme reconnu et sûr, protéger les clés secrètes.

Cette liste n'est pas exhaustive vu l'évolution permanente des actions et des mesures de sécurité à travers le temps.

Après la proposition des différentes actions possibles qui peuvent insuffler une culture sécurité des SI au sein d'une PME, nous allons récapituler ces actions à travers le schéma suivant :

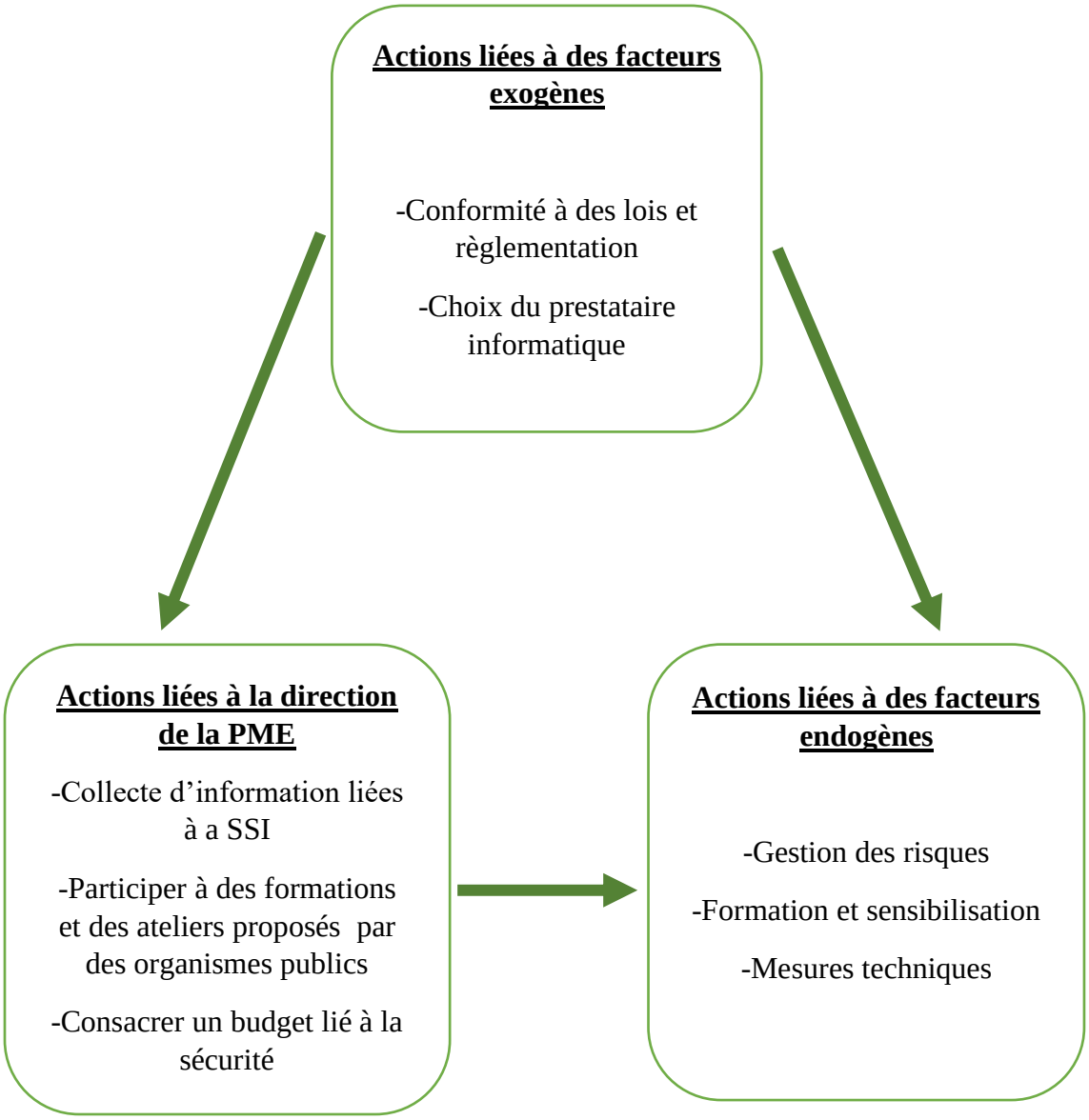


Figure 38 : Processus de la mise en œuvre d'une culture sécurité des SI dans une PME

Synthèse de la section 2

Cette section a été consacrée à la révision de notre modèle de recherche initial avec l'addition des relations et des facteurs (l'âge et le poste de l'utilisateur) qui ont émergé de notre étude qualitative que nous avons discuté sa qualité, au niveau du deuxième titre de cette section. Au niveau du troisième titre nous avons tenter de répondre à notre question de recherche initiale, en proposons des actions à mettre en place afin d'insuffler une culture sécurité des SI au sein des PME.

Conclusion du chapitre 4

A l'issue de la revue de littérature, nous avons élaboré un premier modèle conceptuel avec quatre orientations de recherche, au niveau du chapitre précédent (chapitre 3), nous avons présenté notre étude qualitative et les résultats issus de cette étude et au niveau de ce chapitre, nous avons examiné nos orientations de recherche et nous avons discuté les résultats en les confrontant avec l'examen de la littérature et les résultats des recherche antérieures. Ensuite, nous avons révisé le premier modèle suite aux résultats de l'étude qualitative en proposant un modèle plus affiné que le modèle initial.

Conclusion de la deuxième partie

Cette deuxième partie a été consacrée au déploiement de notre modèle conceptuel à travers une étude qualitative au sein de huit PME. Nous avons approfondi nos résultats par une analyse typologique en réalisant une typologie des PME étudiées, ainsi qu'une typologie des utilisateurs interrogés, pour pouvoir ensuite croiser ces deux dernières entre elles.

Les résultats de cette étude nous ont permis de vérifier nos orientations de recherche qui concernent les facteurs qui influencent la culture sécurité et la relation entre culture sécurité et comportements liés à la sécurité. Nous avons pu valider nos orientations de recherche et nous avons identifié d'autres facteurs qui peuvent jouer un rôle modérateur entre la culture et le comportement, à savoir l'âge et le poste occupé par l'utilisateur. Et nous avons pu identifier une influence des facteurs exogènes (contexte règlementaire et légal, rôle des prestataires de services, secteur d'activité) sur la sensibilité du dirigeant à la sécurité et à son tour, la sensibilité du dirigeant influence les facteurs endogènes (gestion des risques, formation/sensibilisation).

Suite à ces résultats, nous avons révisé notre modèle conceptuel initial, en intégrant les éléments qui ont émergé de notre étude qualitative et nous avons proposé un modèle affiné suite à celle-ci. En appliquant ensuite le processus de la mise en œuvre de la CSSI proposé (figure 38), nous pouvons inculquer une culture de sécurité aux utilisateurs des SI dans les PME.

CONCLUSION GENERALE

Au terme de ce travail, il est essentiel de rappeler les grandes lignes de la démarche (1). Nous présentons ensuite nos principaux résultats (2), puis nous nous penchons sur les apports de la recherche (3). Nous nous interrogeons finalement sur les limites de nos travaux (4) et les perspectives qui s'en dégagent (5).

1. Rappel de la démarche

Suite à des allers retours entre la littérature et l'étude préliminaire qui est l'intervention au sein d'une PME, nous avons constaté dans un premier lieu, que les employés restent le « maillon faible » de la sécurité des SI, d'où la création d'une culture sécurité des SI est nécessaire pour une gestion efficace de la sécurité des systèmes d'information. Dans un second lieu, nous avons constaté que les PME ont généralement peu de moyens et manquent de culture de sécurité des SI. De plus, plusieurs études ont montré leur retard par rapport aux grandes entreprises dans la gestion de la sécurité des SI. Notre étude préliminaire au sein d'une PME en formant et sensibilisant les utilisateurs d'un SI nous a permis d'explorer d'avantage notre objet de recherche, de mieux caractériser le problème enjeu et d'identifier des pistes de réflexion. Nous avons identifié l'existence d'autres facteurs, à part la formation et la sensibilisation, qui elles, peuvent influencer la création d'une culture sécurité des SI. D'où la mise en place d'une culture sécurité des SI qui a été prise en compte dans sa globalité et analysée dans une logique plus systémique, en prenant en compte tous les facteurs qui peuvent l'influencer.

Une revue de littérature nous a permis d'identifier les facteurs qui influencent la culture sécurité et les facteurs qui composent cette culture. Différents modèles ont été construits par les chercheurs afin de comprendre, de cultiver et/ou de mesurer la culture sécurité dans le domaine des SI. Nous avons retenu les facteurs et les composants que nous avons estimé être adaptés au contexte de la PME, ce qui nous a permis de construire notre modèle conceptuel destiné à la gestion de la culture sécurité des SI dans les PME. Après avoir précisé notre cadre conceptuel, nous avons abouti aux orientations de recherche suivantes :

O1. Des facteurs exogènes comme le contexte légal ou la présence d'un prestataire informatique, ou encore l'appartenance à un secteur d'activité sensible à la sécurité influencent positivement la culture sécurité SI dans la PME ;

O2. Des facteurs endogènes comme l'existence d'une évaluation des risques liés à la sécurité des SI ou la réalisation de formations en matière de sécurité des SI influencent positivement la culture sécurité SI de la PME ;

O3. La direction de la PME joue un rôle important dans la création d'une culture sécurité SI ;

O4. L'adoption d'une culture sécurité est favorable à créer un comportement lié à la sécurité.

La question de recherche que nous nous sommes proposés de solutionner est la suivante :

« ***Comment insuffler une culture sécurité des systèmes d'information en PME ?*** ».

Afin de vérifier nos orientations de recherche et répondre à cette question, nous nous sommes positionnés dans une approche interprétativiste, dans la mesure où nous nous privilégions la compréhension de la réalité . Nous avons donc opté pour une méthode qualitative, en premier lieu avec une investigation sur le terrain à partir d'une intervention préliminaire au sein d'une PME, qui nous a permis d'explorer au mieux notre sujet et d'affiner notre problématique de recherche. En deuxième lieu, une étude de cas multiple a été réalisée afin de déployer notre modèle conceptuel et de vérifier nos orientations de recherche. Nos démonstrations et validations se sont appuyées sur une démarche abductive dont notre raisonnement se dessine par une exploration hybride entre exploration théorique et empirique. Le terrain retenu couvre huit PME de différents secteurs (commerce de gros et de détail, service d'aménagement paysager, tri et recyclage etc.) comprenant de 10 à 250 personnes et situées sur la région Ouest de la France. Nous allons maintenant présenter une synthèse de nos principaux résultats de recherche.

2. Synthèse des résultats

L'analyse des données récoltées a été défrichée grâce au logiciel d'analyse de données Nvivo. Nous l'avons approfondie par l'intermédiaire d'un croisement entre les cas étudiés et les acteurs, au sein du même cas. Nous allons maintenant reprendre nos principaux résultats pour chacune des quatre orientations :

O1. Des facteurs exogènes comme le contexte légal ou la présence d'un prestataire informatique ou l'appartenance à un secteur d'activité sensible à la sécurité influencent positivement la culture sécurité SI dans la PME ;

En ce qui concerne le contexte légal et règlementaire, nous avons relevé que l'Etat joue un rôle important en matière de la sécurité des SI, car des lois pourraient obliger les entreprises à mettre en place les actions les plus indispensables. Nous avons identifié un fort besoin d'accompagnement pour les PME, afin de pouvoir mettre en place des actions pour sécuriser leurs SI. Parmi les éléments qui freinent la direction de la PME à mettre en place des mesures de sécurité c'est le manque d'informations, par exemple : quelle démarche mettre en place ? Quels sont les risques et les menaces liés aux SI ? A qui faire confiance au sujet de la sécurité ? Donc, des initiatives de la part du gouvernement ou des organismes publics peuvent améliorer la sensibilité et l'implication des dirigeants, ce qui permet à ces derniers de mettre en place des mesures de sécurité telles que les formations et la sensibilisation à la sécurité, la gestion des risques liés aux SI etc.

A partir de nos études de cas, nous avons identifié qu'il existe plusieurs types de relations entre la PME et son prestataire informatique : une relation de confiance, un rôle de conseil et de support technique, rôle d'RSSI/DPO, confiance limitée, ou une insatisfaction et relation non stable. Les deux PME avec le meilleur niveau de sécurité ont une relation de confiance envers leurs prestataires informatique et les PME avec une relation non stable, une confiance limitée ou une insatisfaction vis-à-vis de leurs prestataires ont un niveau faible à moyen en sécurité.

L'appartenance à un secteur d'activité précis peut déterminer la manière dont les données sont traitées au sein d'une PME, plus le secteur d'activité est sensible à la confidentialité des données, plus le niveau de sécurité sera important par rapport aux secteurs d'activités qui sont moins sensibles à la confidentialité de leurs données, tel que le secteur de commerce.

Notre première orientation s'est avérée vérifiée, puisque les facteurs exogènes influencent directement ou indirectement la culture sécurité de l'utilisateur.

O2. Des facteurs endogènes comme l'existence d'une évaluation des risques liés à la sécurité des SI ou la réalisation de formations en matière de sécurité des SI influencent positivement la culture sécurité SI de la PME ;

A partir de nos résultats, nous avons pu montrer que : plus l'entreprise analyse et évalue les risques liés aux SI et met en place des plans d'actions pour gérer ces risques, plus le niveau de

la culture sécurité des utilisateurs de ses SI augmente. Ce résultat a été approuvé à l'aide de la théorie de la gouvernance des SI (GSI), qui parmi ces deux piliers, nous trouvons la réduction des risques liés aux SI à travers une gestion des risques.

Nous avons montré qu'une formation et une sensibilisation à la sécurité des SI forment un pilier dans la création et l'amélioration d'une culture sécurité des utilisateurs SI. Ce qui a été déjà exploré au niveau de notre partie préliminaire lors de notre intervention.

Notre étude montre aussi que ces deux facteurs (la gestion des risques SI et la formation/sensibilisation) sont mis en place par les dirigeants les plus sensibles à la sécurité.

Notre deuxième orientation a été également vérifiée par le fait que les deux facteurs endogènes (gestion des risques et formation/sensibilisation) jouent une influence positive sur la culture sécurité des utilisateurs des SI.

O3. La direction de la PME joue un rôle important dans la création d'une culture sécurité ;

Nos résultats vérifient cette orientation, d'où un dirigeant sensible au sujet de la sécurité va pouvoir mettre en place des mesures telles que la gestion des risques, les actions de formation/sensibilisation, etc., ce qui va influencer positivement la culture sécurité de ses collaborateurs.

De plus, nous avons montré qu'une implication du dirigeant dans la sécurité est fortement liée au secteur d'activité de sa PME. Par exemple, pour le secteur du commerce de détail, les exigences de sécurité fixées par la direction sont plus faibles, comparées à d'autres secteurs.

O4. L'adoption d'une culture sécurité est favorable à créer un comportement lié à la sécurité.

La plupart des utilisateurs interrogés ont le même niveau en culture sécurité qu'en comportements liés à la sécurité, ceux qui ont un niveau fort en culture sécurité restent sur le niveau 3 (Fort) dans la classification des comportements liés à la sécurité et inversement. Sauf quelques exceptions où leurs niveaux de culture sont différents par rapports à leurs niveaux de comportements, cette différence peut être expliquée par des variables modérateurs tel que l'âge de l'utilisateur ou son poste, ou par le fait qu'un comportement de sécurité par exemple, le changement régulier des mots de passe nécessite un effort de la part de l'utilisateur (du temps,

de la mémorisation, etc.) ce qui peut atténuer leurs comportements liés à la sécurité même s'ils ont conscience de l'importance de telles mesures.

Notre quatrième orientation a donc été partiellement vérifiée, puisque nous avons décelé qu'une culture sécurité positive peut encourager un comportement relatif à la sécurité. Néanmoins, ce n'est pas toujours le cas, nous avons identifié quelques exemples où l'utilisateur, même s'il a une bonne culture sécurité (un niveau élevé), il n'a pas forcément des comportements relatifs à la sécurité (niveau faible à moyen). Une telle différence peut être influencée par l'âge ou le poste de l'utilisateur. Il serait intéressant d'approfondir la piste de recherche concernant les facteurs ou les éléments qui peuvent influencer la relation entre culture et comportements relatifs à la sécurité.

Après la synthèse des résultats de notre recherche liée à chacune des orientations, il nous parait intéressant de rappeler la manière dont nous avons pu estimer le niveau de la culture sécurité de chaque utilisateur, cette estimation ou identification de la culture a été basée sur la théorie des trois niveaux de culture de (Schein, 1985) et chaque niveau a été défini par différentes questions établies au niveau de notre guide d'entretien.

L'ensemble des éléments recueillis et analysés nous a permis de répondre à notre question de recherche initiale :

La mise en place d'une culture sécurité des SI en PME nécessite une analyse systémique, en prenant en compte son contexte (secteur d'activité, contexte règlementaire et légal, la relation avec son prestataire informatique), qui peut jouer une influence notable sur le degré de la sensibilité du dirigeant à la sécurité. Si cette dernière est élevée, le dirigeant a tendance à mettre en place des mesures de sécurité (gestion des risques, formation et sensibilisation à la sécurité) qui vont influencer le niveau de culture sécurité chez les utilisateurs du SI.

La figure ci-après résume le chemin que nous avons parcouru pour répondre à notre question de recherche.

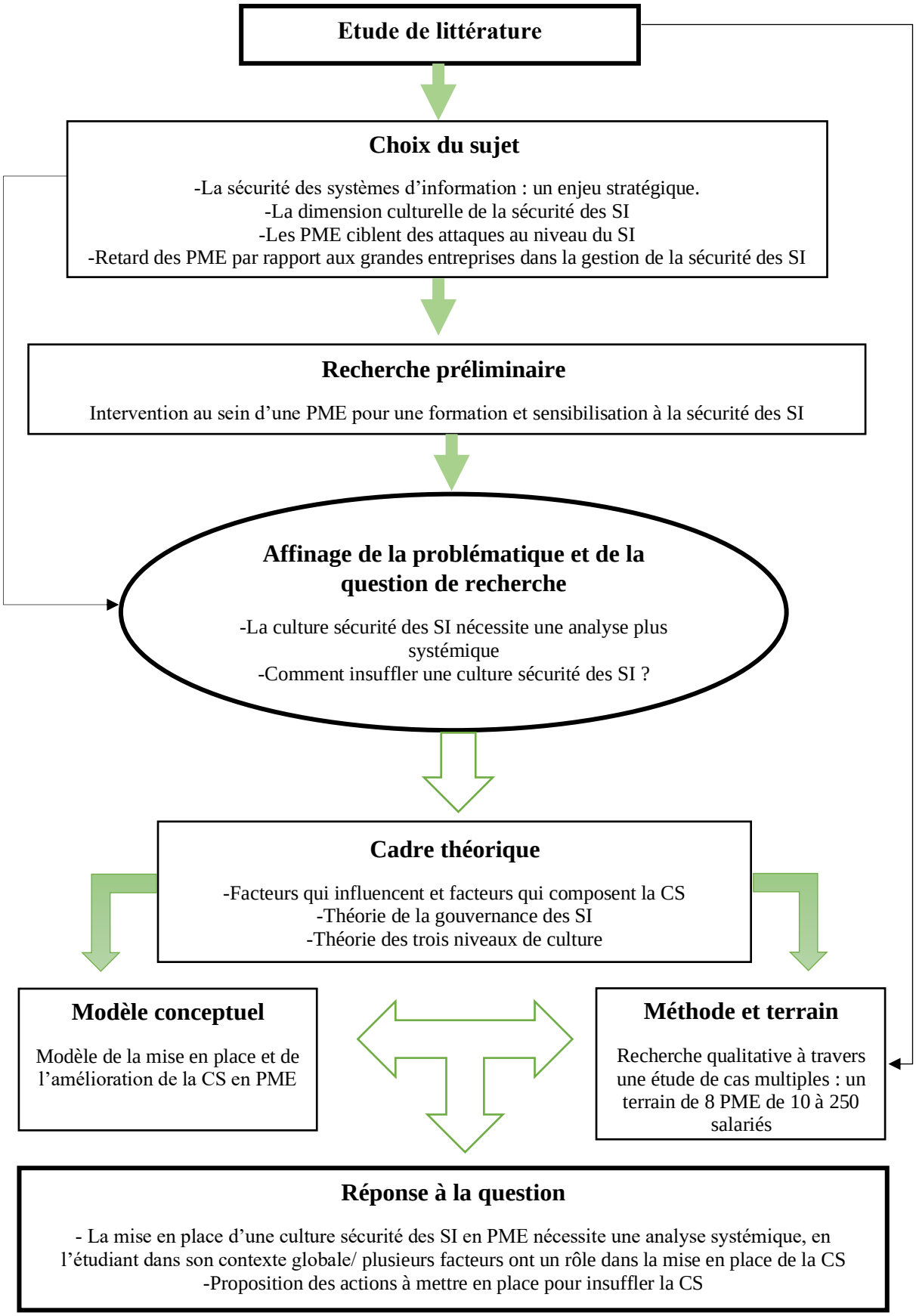


Figure 39 : Le cheminement de la recherche

3. Les apports de la recherche

Les apports de notre recherche se situent au niveau de contributions théoriques et méthodologiques et au niveau d'implications managériales.

1.1 Les contributions théoriques

La majorité des recherches antérieures sur la culture de la sécurité des SI ont fourni beaucoup de connaissances sur la création de culture sécurité. Cependant, la distinction entre les facteurs qui constituent la culture sécurité et les facteurs qui influencent cette culture n'ont pas été examinés de manière approfondie et en particulier dans le cadre des PME ainsi que dans le contexte français. Dans une tentative de combler les lacunes de la recherche et de contribuer à l'ensemble des connaissances existantes, cette recherche offre un modèle de mesure de la culture de sécurité des SI qui fournit également une compréhension initiale de la relation entre les facteurs influençant la culture de sécurité et les facteurs constituant la culture de sécurité.

Notre travail servira de base à une première compréhension de la création ou le développement d'une culture de la sécurité des SI. Cette constitution d'une culture de sécurité des SI est considérée comme une contribution très importante dans le domaine de la recherche sur la culture sécurité des SI, car il y a par ailleurs un manque de définitions et de conceptualisations claires.

Il est essentiel d'évaluer et de comprendre l'existence d'importants facteurs qui influencent la culture de la sécurité des SI, afin de créer une culture de sécurité. Pour atteindre cet objectif, la présente étude a développé un modèle de mesure de la culture de la sécurité des SI afin de comprendre la création d'une telle culture dans les PME françaises. Ce modèle a été construit sur la base des facteurs qui sont spécifiques aux PME, nous avons exclu les facteurs qui concernent dans un premier degré les grandes entreprises, telles que la mise en place d'une politique de sécurité, gestion du changement, etc.

L'apport bénéfique majeur de notre étude réside dans la fourniture d'un modèle adapté à la PME, qui permet à ses entreprises la mise en œuvre et/ou le développement d'une culture sécurité des SI de ses utilisateurs. Ce modèle de culture de sécurité des SI aidera également dans un premier temps à évaluer la relation entre les facteurs qui influencent la culture de sécurité et les facteurs qui constituent ou reflètent la culture de sécurité. Dans un deuxième

temps, ce modèle permet d'examiner la relation entre culture sécurité et comportement relatif à la sécurité accomplie par l'utilisateur du SI. A notre connaissance, peu de travaux ont exploré la relation entre culture sécurité et comportements liés à la sécurité, d'où l'importance de notre recherche qui a exploré cette piste.

Autant que nous sachons, une originalité provient de la mobilisation de la théorie de la gouvernance des systèmes d'information pour évaluer la partie gestion des risques liés aux SI, en déployant le référentiel COBIT (Control Objectives for Information and Related Technology) et plus précisément la partie : « planifier et gérer les risques ». Nous avons démontré que la culture sécurité est un pilier de la gouvernance des SI, où en insufflant une culture sécurité nous gérons au mieux les risques du SI, ce qui va permettre la création de valeur par l'optimisation des coûts à travers la diminution et la gestion des risques liés au SI. A notre connaissance, aucune des recherches antérieures n'a mobilisé cette théorie dans le domaine de la culture sécurité des SI.

En plus de ces contributions, nous avons pu proposer une définition de ce qu'est une culture sécurité des SI. En effet, nous n'avons trouvé aucune définition claire de la culture sécurité des SI au niveau de la littérature. Par ailleurs, il existe une multitude de définitions de la culture sécurité de l'information que nous estimons faire partie de la culture sécurité des SI. Dans ce sens, il nous a donc paru indispensable de proposer notre propre définition.

1.2 Les contributions méthodologiques

Notre travail s'est inscrit dans une démarche interprétativiste et a adapté une méthode de recherche qualitative afin d'étudier la culture sécurité des SI d'une manière systémique et dans son ensemble. La mise en place de cette méthode a permis de réaliser des typologies des PME étudiées ainsi que des profils interrogés et ensuite, un croisement des deux typologies a permis d'analyser et de vérifier nos résultats. Sans oublier notre recherche préliminaire, l'intervention qui nous a permis d'explorer au mieux notre terrain d'investigation et d'aller plus loin dans nos études de cas.

En effet, l'utilisation du modèle de la culture sécurité des SI permet dans un premier temps d'évaluer le niveau de la culture sécurité actuel au sein de la PME et ensuite, de mettre en place ou de renforcer cette culture en jouant sur les facteurs qui l'influencent. Il peut être également utilisé dans l'optique d'une recherche quantitative de relation entre variables. Son utilisation parait possible dans le cadre des PME.

Un autre apport méthodologique de la thèse peut résider dans l'utilisation de certaines fonctionnalités du logiciel NVivo lors de l'analyse des résultats de l'étude qualitative. En effet, si ce logiciel a pour fonction principale de se substituer à la méthode « papier-crayon » pour le codage, par des mécanismes de « glisser-déplacer », nous avons souhaité faire usage de ses autres fonctionnalités. Celles-ci nous ont aidé à éclaircir les facteurs identifiés au niveau de la littérature et facilité la réalisation des typologies (entreprises, utilisateurs).

3.3 Les implications managériales

Le modèle de recherche offre un certain nombre d'observations qui peuvent guider les directeurs de PME dans la création et l'amélioration d'une culture sécurité de leurs SI. Les observations sont les suivantes :

Notre travail peut servir à mettre en place des campagnes de sensibilisation ou de formations adaptées aux utilisateurs des SI. Il s'agirait de leur donner un enseignement de base en S.I., de les sensibiliser aux problématiques relatives à la SSI en les aidant par exemple de mieux connaitre et comprendre les principaux risques auxquels ils auront à faire face, ainsi que les conséquences de certains sinistres liés à leurs postes et liés au secteur d'activité de la PME. Les facteurs qui influencent la culture sécurité de l'utilisateur donneront plus d'impact à ces sensibilisations et formations.

La présente étude aide les responsables et surtout le dirigeant de la PME, à développer des aspects importants de la sécurité des SI qui conduiront par la suite à la création d'une culture de la sécurité. Le modèle de recherche donne à la direction les moyens de mettre en œuvre des approches de gestion de la sécurité des SI. Ces approches fourniront un point de référence unique pour la gestion de la SSI, afin d'inculquer un niveau acceptable de culture de sécurité.

Cette recherche aide à minimiser les menaces que les comportements des employés posent à la protection des SI de la PME. Le modèle établi facilite la compréhension de la culture sécurité et les éléments susceptibles de renforcer cette culture. Par la compréhension des facteurs qui composent la culture sécurité tels que : propriété, conscience et conformité, les décisions des dirigeants peuvent aider à diriger l'interaction des utilisateurs avec les mesures de sécurité afin de contribuer à la protection du SI de l'entreprise.

Notre étude, offre un éclairage sur le rôle qui peut être joué par les pouvoirs publics en matière de sécurité des SI auprès des PME, surtout que ces entreprises expriment un fort besoin d'accompagnement sur le sujet de la sécurité : quelle démarche mettre en place ? Comment

faire face aux risques et aux menaces ? A qui faire confiance sur le sujet de la sécurité ? Par la distribution de brochures de sensibilisation à la sécurité des SI destinées aux PME et la conduite d'une analyse comparative de la sécurité des SI des PME en France et entre régions, par exemple. Propositions des mesures de sécurité adaptées aux PME, selon leur secteur d'activité, selon leurs ressources disponibles (financières, techniques, humaines, matérielles).

Pour aider les PME Françaises, des exemples de scénarios de risques de sécurité peuvent être développés à partir des ressources existantes. Celles-ci peuvent être formulées en termes de protection contre la perte d'actifs, afin de mieux attirer les PME. Les initiatives devraient cibler également le contexte national. Par exemple, la France a une culture d'aversion au risque et donc les brochures et autres initiatives devraient viser à répondre à cette caractéristique « de résistance aux risques ».

En ce qui concerne les prestataires de services informatiques, ils peuvent jouer un rôle dans la sensibilisation des PME à la sécurité, en proposant des solutions et des technologies qui peuvent sécuriser les SI. Ces solutions doivent être adaptées au contexte de la PME, en prenant en compte les limites budgétaires, le manque de connaissances techniques et technologiques, etc., pour pouvoir gagner leur confiance et de leur fournir une véritable valeur ajoutée dans la gestion de la sécurité de leurs SI.

2. Les limites et les prolongements de la recherche

Si les apports de ce travail sont à nos yeux bien réels, la présente recherche n'est en effet pas sans limites. Les points suivants résument les limites de notre recherche et chacune des limites identifiées propose des prolongements à notre travail :

Notre recherche est confrontée aux limites liées à la méthodologie qualitative adoptée pour étudier la culture sécurité, d'où le problème de généralisation des résultats, du fait de conclusions basées sur huit cas et 32 entretiens. Une étude de type quantitatif pourra vérifier et affiner ces résultats, si nécessaire.

Les résultats de la recherche ne peuvent être généralisés à d'autres pays, puisque la culture nationale est susceptible d'affecter la culture et les comportements relatifs à la sécurité des SI, comme les Etats unis qui ont un système qui incite à la prise de risque, ou l'Australie qui a une culture de « laissez-faire ».

Une autre limite due aux caractéristiques des PME étudiées, où toutes les PME disposent d'un prestataire informatique, activent dans des secteurs d'activités similaires (Commerce, Transformation et conservation, Tri et recyclage) et situées dans la même région géographique. L'étude d'autres cas hétérogènes, telles que des PME qui ne font pas recours à des prestataires informatiques, des PME du secteur informatique, ou par exemple d'identifier les plus sensibles à la confidentialité des données ainsi que celles dépendant fortement de la disponibilité et de l'intégrité de leurs informations (centre d'appel, par exemple), permettent de vérifier quelles différences peuvent apparaître au sujet de la culture et des comportements relatifs à la sécurité des systèmes d'information.

Le cadre manque d'éléments spécifiques applicables uniquement aux PME (par opposition aux grandes entreprises). Nous soupçonnons que certains des éléments inclus sont plus fortement influents dans les PME, comme la sensibilité du dirigeant à la sécurité. Des recherches futures pourront explorer cette piste.

Le nombre de cas étudiés a été limité à huit, ce qui pour Yin (1994) est considéré comme suffisant pour en tirer des enseignements. A ce stade de recherche, la généralisation quantitative des résultats n'est pas possible. Il serait avantageux de pousser plus loin l'étude des facteurs qui influencent ainsi que ceux qui constituent la culture sécurité par le biais d'une étude quantitative et d'identifier plus précisément quels facteurs vont agir le plus sur la culture sécurité et ceux qui vont agir le plus sur les comportements relatifs à la sécurité. Et de vérifier quelle est la relation entre culture sécurité et comportements liés à la sécurité, ainsi que l'influence de l'âge et du poste de l'utilisateur du SI sur cette dernière.

Le cadre a été élaboré dans le contexte Français. Il est clair que d'autres pays peuvent être intéressés par la valeur potentielle du cadre, qui devrait donc être explorée dans d'autres paramètres nationaux. Cela sera intéressant de mener une analyse comparative entre les PME françaises et les PME au sein d'autres pays de l'Union Européenne.

Lors de prochaines études, il serait souhaitable de mieux prendre en compte différents secteurs d'activité afin de comprendre la différence entre les PME techniques qui employaient du personnel possédant des connaissances dans le domaine informatique (secteur informatique et télécommunication), les PME sensibles à la sécurité des données (aéronautique, nucléaire, etc.) et les PME les moins sensibles à la sécurité des données (commerce, industrie, etc.).

La voie juridique nous semble prometteuse, car des lois pourraient obliger les dirigeants - même les moins sensibles à la sécurité - à mettre en place les actions les plus indispensables. A titre

d’exemple, le règlement général sur la protection des données (RGPD), même s’il semble lourd à mettre en place par les PME, néanmoins, sa mise en place peut renforcer la culture sécurité au sein de la PME. Ceci pourrait permettre à terme la création d'une méthode allégée adaptée aux PME, peu chère et facile à mettre en place.

Il serait intéressant en mobilisant la théorie de la gouvernance des SI, de montrer si une amélioration de la culture et des comportements liés à la sécurité entraîne une création de valeur et contribue à la performance de l’entreprise, en utilisant des indicateurs de performance tels que les taux d'incidents liés au SI, nombre de virus et de codes malveillants bloqués, pourcentage d’utilisateurs qui ne se conforment pas aux exigences de sécurité mises en place.

Des études considérant les effets modérateurs de certaines variables sociodémographiques comme l’âge, le sexe, le niveau de formation, les problèmes vécus et le poste de l’utilisateur. Ces critères de contingence offrent la possibilité de mieux cerner les mécanismes de régulation des déterminants de la culture sécurité et des comportements relatifs à la sécurité des SI.

La piste de la formation et sensibilisation nous paraît très prometteuse, car la culture sécurité ne peut pas se réduire à une problématique de carotte et de bâton. D’ailleurs, des recherches récentes (Pattinson et al. 2018 ; Van Bavel et al. 2019 ; Dincelli et Chengalur-Smith, 2020), montrent que les utilisateurs finaux veulent être des participants autonomes, compétents, motivés et actifs dans le développement d'environnements sécurisés. Il a été démontré aussi que des interventions gamifiées, l’utilisation des méthodes de ‘’coup de pouce’’ ou ‘’Nudge’’ dans le contexte de la sécurité des S.I. améliorent les comportements des participants (utilisation des technologies sécurisées, choix des mots de passe solides). Néanmoins à notre connaissance, ces méthodes ont été déployées dans les grandes organisations, mais non encore dans le contexte des PME. D’où les questions suivantes qui pourraient se poser : Dans quelle mesure une adaptation de la formation/sensibilisation aux préférences des utilisateurs des SI en PME peut-elle améliorer leur culture sécurité ? A quel niveau, la mobilisation de la théorie du ‘’Nudge’’ peut améliorer la culture sécurité des utilisateurs de SI dans la PME ?

Pour conclure, les résultats de cette étude sont riches et pertinents et contribuent, in fine, à améliorer la compréhension des déterminants de la culture sécurité dans le domaine des SI. Par ailleurs, dans l’optique de cultiver une culture sécurité et améliorer les comportements liés à la sécurité des utilisateurs du SI, des dirigeants de PME, des institutions publiques et/ou des prestataires informatiques peuvent être intéressés par les résultats de cette thèse.

Bibliographie

A

- Absil, M. (2014*), Les discours sur la notion de vulnérabilité,* psychiatries.be, Centre Franco Basaglia, 1ère édition, 7 pages.

- Achchab, B., & Harrizi, D. (2013), « Les défis de l'intelligence économique au Maroc », *La Revue Gestion et Organisation, 5*(2), 130–137.

- Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y., Wilson, S. (2017), « Nudges for privacy and security: Understanding and assisting users' choices online », *ACM Computing Surveys*, *50*(3), 1–41.

- Acs ZJ, Gerlowski DA. (1996), *Manegerial economics and organization*, Prentice Hall; 1996, 464 pages.

- Adams A., Sasse M.A., (1999), « Users are not the enemy », Communications of the ACM, Vol.42, n°12, pp. 40-46;

- Adams J.S., (1963), « Towards an understanding of inequity », *Journal of abnormal and normal social psychology* (67), pp. 422-436;

- Adams J.S., (1965), *Inequity in social exchange*, in Advances in experimental psychology, 2, 267-299.

- Aggeri F. (2016), *La recherche-intervention : fondements et pratiques. Jérome Barthélemy et Nicolas Mottis. A la pointe du management. Ce que la recherche apporte au manager*, Dunod, pp.79-100, 2016.

- Agnew R., (1995), « Testing the leading crime theories: an alternative strategy focusing on motivational process », *Journal of research in crime and delinquency*, (32: 4), pp. 363-398.

- Ajzen I., (1991), « The Theory of Planned Behavior », *Organizational Behavior and Human Decision Processes,* (50:2), pp. 179-211.

- Ajzen I., Fishbein M., (1980), *Understanding attitudes and predicting social behaviour*, Prentice hall, Englewood cliffs, NJ, USA.

- Akers R.L., (1985), *Deviant Behaviour: A Social Learning Approach*, Wadsworth, Belmont, Ca, USA, 421 pages.

- Akers R.L., (1997), *Criminological Theories: Introduction and Evaluation*, 2nd ed, Roxbury Publishing, Los Angeles, Ca, USA.

- Akers R.L, Krohn, M.D, Lanza-Kaduce, L., Radosevich, M., (1979), « Social learning and deviant behaviour: a specific test of a general theory », *American Sociological Review*, Vol. 44,pp. 636-655.

- Akhyari, N., Ruzaini, A. A., Rashid, A. H. (2018), « Information Security Culture Guidelines To Improbe Employee'S Security Behavior: a Review of Empirical Studies », *Journal of Fundamental and Applied Sciences*, *10*(2S), 258–283.

- Albarello L., (2004), *Apprendre à chercher : l'acteur social et la recherche scientifique*, Bruxelles, De Boeck, 2004.

- Alfawaz, S., Nelson, K., et Mohannak, K. (2010), « Information security culture : a behaviour compliance conceptual framework », Australasian Information Security Conference (AISC), 2010, Brisbane, Australia.

- AlHogail, A., Mirza, A. (2015), « Organizational Information Security Culture Assessment », The 2015 International Conference on Security and Management, October, 286–292.

- Alhogail, A., Mirza, A., Bakry, S.H. (2015), « A comprehensive human factor framework for Information Security in organisations », *Journal of Theoretical and Applied Information Technology*, Vol. 78, No. 2, pp201.

- Alhogail, A., Mirza, A. (2014), « Information security culture: A definition and a literature review », *Computer Applications and Information Systems*, pp. 1-7.

- Alhogail, A., Mirza, A. (2014), « A framework of information security culture change », *Journal of Theoretical and Applied Information Technology*, Vol. 64 No. 2, pp. 540–549.

- Allard-Poesi, F. (2003), *Coder les données*. in Y. Giordano (Dir.), Conduire un projet de recherche, une perspective qualitative, Caen : EMS, 2003, pp. 245-290.

- Alnatheer, M. and Nelson, K. (2009), « Proposed framework for understanding information security culture and practices in the Saudi context », 7th Australian Information Security Management Conference, Edith Cowan University, Perth, 1-3 December, pp. 5-17.

- Alnatheer, M. A. (2012), « Understanding and Measuring Information Security Culture in Developing Countries : Case of Saudi Arabia », *Computer Systems and Information Technology*, *9*(14), 897–912.

- Alnatheer, M., Chan, T., Nelson, K. (2012), « Understanding And Measuring Information Security Culture », Pacific Asia Conference on Information Systems, pp144.

- Alnatheer, M. (2014), « A Conceptual Model to Understand Information Security Culture » *International Journal of Social Science and Humanity*, Vol. 4, No. 2, March 2014.

- Alqahtani, H. S. (2016), « Latest Trends and Future Directions of Cyber Security », *Information Systems*. *6*(11), 9–14.

- Amrin, N., Hartel, P., Junger, M., Leijtens, A. (2014). The Impact of Cyber Security on SMEs, University of twente.

- Andersen Consulting, (2000), « La sensibilisation des collaborateurs à la sécurité des informations », Novembre 2000.

- Andreani J.C, (1998), « L'interview qualitative en marketing », *Revue Française de Marketing*, 168-169,3-4, 1998.

- Anderson, B. B., Vance, A., Kirwan, C. B., Eargle, D., Jenkins, J. L. (2016), « How users perceive and respond to security messages: A NeuroIS research agenda and empirical study », *European Journal of Information Systems*, *25*(4), 364–390.

- Anderson, E. E., & Choobineh, J. (2008), « Enterprise information security strategies », *Computers & Security*, *27*(1–2), 22–29.

- Archimbaud, J.L., Longeon, R., (1999), « Guide de la sécurité des systèmes d'information à l'usage des directeurs », *CNRS*, Paris.

- Ashenden, D. (2008), « Information Security management: A human challenge? », *Information Security Technical Report*, *13*(4), 195–201.

- Ashenden, D., Sasse, A. (2013), « CISOs and organisational culture: Their own worst enemy? », *Computers and Security*, Vol. 39 No. 2013, pp. 396–405.

- Astakhova, L.V. (2014). « The Concept of the Information Security Culture », *Scientific and Technical Information Processing*, vol. 41, no 1, p. 22-28.

- Autissier, D., Delaye, V. (2008), *Mesurer la performance du système d ' information*, Collection Les baromètres de la performance, 216 pages.

- Avenier M. J., (1989), « Méthodes de terrain et recherche en management stratégique » , *Economies et Sociétés*, N°14, 199-218.

- Ayse C. (1998), « Analyser la sécurité : Dillon, Waever, Williams et les autres », *Cultures & Conflits*, 31-32, printemps-été 1998.

B

- Bardin, L. (1998). L'analyse de contenu. Paris : Presses universitaires de France (9e éd.).
- Barlatier, P-J. (2018), *Les études de cas*, Les méthodes de recherche du DBA , Edition: Collection Business Science Institute.
- Barlette, Y. (2005). « L'implication des décideurs détermine les comportements sécuritaires des acteurs en PME ». AIM 2005, Toulouse, August.
- Barlette Y. (2006), Les comportements sécuritaires des acteurs dans les Systèmes d'Information des PME, Thèse de doctorat en sciences de gestion de l'université de Montpelier I, 383 pages.
- Barlette, Y. (2007). Les comportements sécuritaires des acteurs dans les systèmes d'information des PME. 12th International Conference of the Association Information and Management *2007,* AIM *2007*.
- Barlette, Y. (2008), « Une étude des comportements liés à la sécurité des systèmes d'information en PME », *Systèmes d'information & Management, 13*(4), 7.
- Barlette, Y. (2009). Vers une implication et une action des dirigeants de PME dans la sécurité de leur système d'information. *14th International Conference of the Association Information and Management 2009, AIM 2009, August*.
- 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, p. 119-140. IGI Global, USA.
- Barlette, Y. (2012), «Implication et Action des Dirigeants: Quelles Pistes pour Améliorer la Sécurité de L'information en PME?» *Systèmes d'Information & Management*, Vol. 17, n°2, p. 115-149.
- Barlette, Y., Gundolf, K., & Jaouen, A. (2015), « Toward a better understanding of SMB CEOs' information security behavior: Insights from threat or coping appraisal ». 20th Symposium of the Association Information and Management 2015, *AIM 2015*, *5*(1), 5–17.
- Barlette, Y., Gundolf, K., Jaouen, A. (2017), « CEOs' information security behavior in SMEs: Does ownership matter? », *Systèmes d'information & management,* V. 22, Issue 3.
- Barlette, Y., Jaouan, A., (2019), « Information security in SMEs: determinants of CEOs' protective and supportive behaviors », *Système d'information et Management*, N° 3 – VOL. 24, 2019.

- Barlow, J. B., Warkentin, M., Ormond, D., Dennis, A. R. (2018), « Don't even think about it! the effets of antineutralization, informational, and normative communication on information security compliance », *Journal of the Association for Information Systems, 19*(8), 689–715.

- Barreyre, P.Y. (1967), « L'horizon économique des petites et moyennes entreprises », *Thèse pour le doctorat de Sciences Economiques*, Université de Grenoble, 480 p.

- Barton, K.A., Tejay, G., Lane, M., Terrell, S. (2016), «Information System Security Commitment: A Study of External Influences on Senior Management», *Computers & Security*, Vol. 59, p. 9-25.

- Baumard P., Donada C., Ibert J., Xuereb J.M., (1999), "La collecte des données et la gestion de leurs sources", in Raymond-Alain Thiétart et coll., *Méthodes de recherche en management*, Paris, Dunod, pp. 224-256.

- Bayad, M., Nebenhaus D. (1994), « Recherches sur la GRH en PME : proposition en vue d'un modèle théorique », *communication au Vème Congrès de l'AGRH*, Montpellier, p. 235-242.

- Bazeley, P. (2007). Going further In Qualitative data analysis with NVivo, *Sage Publications*, p.177-209.

- Blakley B., McDemott E., Geer D., (2001), « Information security is information risk management », Proceedings of the 2001 workshop on New security paradigms, pages 97-104.

- Bellier, F., Gregoire, F., Donadey, F. (2002), « Etude du concept de vulnérabilité : une notion d'avenir », *projet cindynique*, Ecole Nationale des Mines, Saint-Etienne.

- Bennis, W.G., *Le développement des organisations*, Paris, Dalloz, 1975, 100 pages.

- Benghozi, J-P. (2001). « Technologies de l'information et organisation : de la tentation de la flexibilité à la centralisation ». *Revue gestion* 2000, 2(mars-avril), 61-80.

- Bergeron P., Hiller C. A., (2002), « Competitive intelligence », *Annual Review of Information Science and Technology*, Volume36, Issue1, P 353-390.

- Besnard D., Boissières I., Daniellou F., Villena J., (2017), *La culture de sécurité : comprendre pour agir*, Edition Institut pour une culture de sécurité industrielle, 130 pages.

- Besson, B., Possin, J. (2006), « L'intelligence des risques », *Market Management*, 3(3), 104-120.

- Bhattacharya, D. (2011), «Leadership Styles and Information Security in Small Businesses», *Information Management & Computer Security*, Vol. 19, n°5, p. 300-312.

- Bidan, M., Trinquecoste, J.-F. (2010), « Gouvernance et innovation à l'épreuve des technologies de l'information », *Management & Avenir*, Vol. 4, n° 34, p. 125- 127.

- Bidan, M., Rowe, F., Truex, D. (2012). « An empirical study of IS architectures in french SMEs : integration approaches ». *European Journal of Information Systems*, 21(3), 287-302.

- Bilal K., (2011), « Effectiveness of information security awareness methods based on psychological theories », *African Journal of Business Management*, *5*(26), 10862–10868.

- Blackwell, P., Shehab, E.M., Kay, J.M. (2006). « An effective decision-support framework for implementing enterprise information systems within SMEs ». *International Journal of Production Research*, 44(1), 3533-3552.

- Blanchet, A., Gotman, A. (2010). L'entretien: L'enquête et ses méthodes. *Paris: Armand Colin*.

- Blakley, B. McDemott, E. Geer, D. (2001), « Information security is information risk management ». Conférence paper in Proceedings New Security Paradigms Workshop.

- Blake R. R. ; Mouton J.S., (1964), *The Managerial Grid*, Houston, TX; Gulf.

- Bodet, C., Lamarche, T. (2007), « La responsabilité sociale des entreprises comme innovation institutionnelle. Une lecture régulationniste », *Revue de la régulation*, n° 1, juin.

- Boer, H., Seydel, E. R. (1996), « Protection motivation theory », *Predicting Health Behavior: Research and Practice with Social Cognition Models* (pp. 95–120).

- 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.

- Bournois, F., Romani P.J., (2000), *L'intelligence économique et stratégique dans les entreprises françaises*, Economica, Paris.

- Box D., Pottas D., (2013), « Improving information security behaviour in the healthcare context », International Conference on Health and Social Care Information Systems and Technologies.

- Brandao R. (1993), IT-Sicherheitskultur im Unternehmen, diploma thesis IFI. Zürich: Universität Zürich, 1994, pp. 110.

- Brodeur, J. (2006). « Le risque et la menace ». *Canadian Journal of Criminology and Criminal Justice*, 48(3), 491-498.

- Bruhn, M. (1999). Internes Marketing als Forschungsgebiet der Marketingwissenschaft. Eine Einführung in die theoretischen und praktischen Probleme. In: M. Bruhn, Ed. Internes Marketing: Integration der Kunden- und Mitarbeiterorientierung. Grundlagen Implementierung - Praxisbeispiele. *Wiesbaden, Gabler*. 2. Auflage: 15-44.

- Bruce G., Dempsey R., (1997), « Security in Distributed Computing - Did You Lock the Door ? », *Hewlett Packard Company*, Palo Alto, USA;

- Brytting, T. (1991), « Organizing in the small growing firm : a grounded theory approach », *The Economic Research Institute/EFI*, Stockholm, 238p.

- Brooksbank, R. (1991), « Defining the small business : a new classification of company size », *Entrepreneurship and regional development*, n°3, p. 17-31.

- Bridges W. (2003), Managing transitions: Making the most of change, 2. New York, NY: Da Capo P; 2003.

- Bruno C., (2010), *Conceptualisation de la Gouvernance des Systèmes d'Information : Structure et Démarche pour la Construction des Systèmes d'Information de Gouvernance* , Thèse de doctorat, Université Panthéon-Sorbonne - Paris I, 2010.

- Bulgurcu, B., Cavusoglu, H., Benbasat, I. (2010), « Information Security Policy Compliance: AnEmpirical Study of Rationality-Based Beliefs and Information Security Awareness », *MIS Quarterly*, 34 (3), 523-548.

- Buzan, B. (1993)., *Societal Security, State Security, and Internationalisation*, In O. Waever, B. Buzan, M. Kelstrup and P. Lemaitre (Eds.), Identity, Migration and the New Security Agenda in Europe (pp. 41–58). London: Pinter.

- Buzan, B., Kelstrup, M., P. Lemaitre (1993), *Identity, Migration and the New Security Agenda in Europe*, London, 1993, p. 57.

C

- Cappelletti, L. (2010), « La recherche-intervention: quels usages en contrôle de gestion? », Crises et nouvelles problématiques de la Valeur, May 2010, Nice, France.

- Cazier, J.A., Jensen, A.S., Dave, D.S. (2008), « The Impact of Consumer Perceptions of Information Privacy and Security Risks on the Adoption of Residual RFID Technologies », *Communications of the Association for Information Systems*, Vol. 23 , Article 14.

- Chamfrault T., Durand C., (2006), *ITIL et la gestion des services*, Ed. Dunod, 2006.

- Chanal, V, Lesca, H, Martinet, C.A., (1997), « Vers une ingénierie de la recherche en gestion », *Revue Française de Gestion*, n°116, nov.-déc., pp.41-51.

- Chante, A. (2010), « La culture de l'information, un domaine de débats conceptuels ». *Les Enjeux de l'information et de La Communication*, *2010*(1), 33.

- Charndra, A., Calderor, T. (2005), « Challenges and Constraints to the Diffusion of Biometrics in Information Systems », *Communications of the ACM*, Vol. 48, n° 12, p. 101-106.

- Chen, Y., Ramamurthy, K. , Wen, K.-W. (2015). « Impacts of Comprehensive Information Security Programs on Information Security Culture ». *Journal of Computer Information Systems*, 55(3), 11–19.

- Chen, Y., Zahedi, F. M. (2016). « Research Note Individual's Internet Security Perceptions and Behaviors : Polycontextual Contrasts Between the U Nited S Tates and China ». *MIS Quarterly*, *40*(1), 205–222.

- Chia, P.A., Maynard, S.B. , Ruighaver, A.B. (2002), « Understanding organisational security culture », Sixth Pacific Asia Conference on Information Systems, pp731-740.

- Chrissis M. B., Konrad M., Shrum S., (2008), *CMMI 2e édition - Guide des bonnes pratiques pour l'amélioration des processus - CMMI ® pour le développement, version 1.2* , Pearson Education France, 2008, ISBN 978-2-7440-7304-5.

- Churchill, G.A. (1979), « A Paradigm for Developing Better Measure of Marketing Constructs », *Journal of Marketing Research*, Vol.16, n°1, pp. 63-73.

- Cohen, E. (1989), *Epistémologie de la gestion*, Encyclopédie de Gestion, Paris, Ed Economica, p. 1055-1074.

- Colella A., Castiglione A., Santis A., The Role of Trust and Co-partnership in the Societal Digital Security Culture Approach, in International Conference on Intelligent Networking and Collaborative Systems, 2014, pp. 350–355.

- Claudepierre B., (2010) , *Conceptualisation de la Gouvernance des Systèmes d'Information : Structure et Démarche pour la Construction des Systèmes d'Information de Gouvernance*, Thèse de doctorat, Université Panthéon-Sorbonne - Paris I, 2010.

- Clusif. (2012). *Menaces informatiques et pratiques de sécurité en France*, Club de la sécurité informatique Français, édition Juin 2012.

- Connolly, L. and Lang, M. (2012), « Investigation of cultural aspects within information systems security research », The 7th International Conference for Internet Technology and Secured Transactions (ICITST 2012), IEEE Digital Library, London, pp. 105-111.

- Connolly L, Y., Lang, M., Gathegi J., Doug J. Tygar D, J., (2017), « Organisational Culture, Procedural Countermeasures, and Employee Security Behaviour: A Qualitative Stud », *Information & Computer Security*, Vol. 25.

- Coutelle, P., (2005), Introduction aux méthodes qualitatives en Sciences de Gestion, Cours du CEFAG – séminaire d'études qualitatives 2005, pp.1–20.

- CPME (2019), *La cybersécurité des entreprises (-50 salariés) : Enquête*, Janvier 2019.

- Cragg, P., Caldeira, M., Ward, J. (2011), «Organizational Information Systems Competences in Small and Medium-Sized Enterprises», *Information & Management*, Vol. 48, n°8, p. 353 363.

- Croteau, A. M., Bergeron, F. (2001), « An information technology trilogy: Business strategy, technological deployment and organizational performance », *Journal of Strategic Information Systems*, *10*(2), 77–99.

- Croteau, A. M., Bergeron, F., Raymond, L. (2001), « Comportements stratégiques , choix et gestion des systèmes d'information : contribution à la performance », *Système d'Information et Management*, *6*(4), 5–26.

- Cucchi, A. (2011). « Management de la sécurité de l'information, mise en œuvre, évaluation et pilotage de la sécurité de l'information dans les organisations », Nathalie Dagorn. *Systèmes d'information & Management*, *16*(4), 104.

- Curvalle B., Torrès O., (1998), *Le système EDI/JAT condamne-t-il les PME*, in Torres O. (Éd.), PME : De nouvelles approches, *Economica*, Paris.

D

- D'Amboise, G et Maldowney M. (1988), « Management theory for small business : attempts and requirements », *Academy of Management Review*, Vol 13, n°2, p. 226-240.

- D'Amboise, G et Plante G. (1987), « La recherche sur la PME : quelques voies pour des relations efficaces entre chercheurs et dirigeants », *Revue de Gestion des Petites et Moyennes organisations*, Vol 3, n°1, p. 44-50.

- D'Amboise, G. (1989), *La PME canadienne : situation et défis*, Québec, Les Presses de l'Université Laval.

- D'Arcy J, Greene G. (2009), The multifaceted nature of security culture and its influence on end user behavior, In International Workshop on Information Systems Security Research, 2009, pp. 145-157.

- D'Arcy J, Greene G. (2014), « Security culture and the employment relationship as drivers of employees' security compliance », *Information Management and Computer Security*, , Vol. 22 Iss 5 pp. 474 – 489.

- D'Arcy, J., Hovav, A., and Galletta, D. (2009), « User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse », *Information Systems Research*, 20 (1), pp. 79– 98.

- Da Veiga, A. (2015), « An information security training and awareness approach (ISTAAP) to instil an information security-positive culture », Proceedings of the 9th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2015, *Haisa*, 95–107.

- Da Veiga, A. (2015), « The influence of information security policies on information security culture: Illustrated through a case study », *Proceedings of the 9th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2015*, *Haisa*, 22–33.

- Da Veiga A (2018), « An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture », *Information & Computer Security*, Vol. 12, Issue 5, 2018.

- Da Veiga A, Eloff (2010), « A framework and assessment instrument for information security culture », *computers & security* 29 (2010) 196-207.

- Da Veiga A, Eloff JHP. (2007), « An information security governance framework ». *Information Systems Management* 2007;24(4).

- Da Veiga A, Martins N, Eloff JHP. (2007), « Information security culture – validation of an assessment instrument ». *Southern African Business Review* 2007;11(1):146–66.

- Da Veiga A., Martins, N. (2014), Information Security Culture: A Comparative Analysis of Four Assessments, European Conference on Information Management and Evaluation, At Ghent, Belgium, V 8.

- Da Veiga A., Martins, N. (2015), « Information security culture and information protection culture: A validated assessment instrument », *computer law & security review* 31 (2015) 243 -256.

- Da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers and Security*, *70*, 72–94.

- Dagorn, N. (2008), « Politiques en matière de sécurité des systèmes d'information inter-organisationnels : une enquête dans dix grandes entreprises ». *Systèmes d'information & Management*, *13*(2), 97.

- Dagorn, N., Poussing, N. (2012), « Engagement et pratiques des organisations en matière de gouvernance de la sécurité de l'information », In *Systèmes d'information & management* Vol. 17, Issue 1.

- Dahbur, K., Bashabsheh, Z., Bashabsheh, D. (2017), « Assessment of Security Awareness: A Qualitative and Quantitative Study » , *International Management Review, 13*(1), 37.

- Dandridge, T. C. (1979), « Children are not "little grownp-ups" : small business needs its own organizational theory », *Journal of Small Business Management*, Vol 17, n°2, p. 53-57.

- Dandrige, T. et Levenburg, N.M. (2000). « High-tech potential ? An exploratory study of very small firms' usage of the Internet ». *International Small Business Journal*, 18(2), 81-91.

- Dario B., (2009), Théories des relations internationales, Edition Presses de Sciences Po, 696 p, 2009.

- David, A. (2000a), *Logique, épistémologie et méthodologie en sciences de gestion : trois hypothèses revisitées*, Les Nouvelles Fondations des Sciences de Gestion, Paris Vuibert, 83-109.

- David, A. (2000b), *La recherche intervention, un cadre général pour les sciences de gestion ?*, IXème Conférence de l'AIMS, Montpellier, 24-26 mai.

- David, A., (2005). « Des rapports entre généralisation et actionnabilité: le statut des connaissances dans les études de cas », 6ème Congrès Européen de Science des Systèmes, Paris, pp. 1–17.

- Davis F.D., Bagozzi, R. P., Warshaw, P. R., (1989), « User Acceptance of Computer Technology: A Comparison of Two Theoretical Models," *Management Science* (35:8), pp. 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* (22:14), pp. 1111-1132;

- De Ketele, J. M., Roegiers, X. (1996). « Méthodologie du recueil d'informations: fondements des méthodes d'observations, de questionnaires, d'interviews et d'études de documents ». De Boeck Université.

- Deal T.E.., Kennedy A. (1982), *Corporate Cultures: The Rites and Rituals of Corporate Life*, Reading, MA: AddisonWestey.

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

- Deci E.L., Ryan R.M., (1985), *Intrinsic motivation and self-determination in human development*, Plenum press, NY, USA;

- Del Bayle J.L., (2000), *Initiation aux méthodes des sciences sociales*, Paris: L'Harmattan.

- Deloche de Noyelle. G., Westercamp P. (1971), «Les trois composantes d'un MIS », *Informatique et gestion*, 30, septembre 1971.

- DeLone, W. H., McLean, E. R. (2003), « The DeLone and McLean Model of Information Systems Success: ATen-Update », *Journal of Management Information Systems, 19*(4), 9-30.

- Deschenaux, F. (2007). *Guide d'introduction au logiciel QSR NVivo7*. Les cahiers pédagogiques de l'Association pour la recherche qualitative.

- Detert J. R., Schroeder R. G., Mauriel J. J. (2000), « A Framework for Linking Culture and Improvement Initiatives in Organizations », *Academy of Management Review* V. 25, No. 4.

- Dillon M., (1996), « Politics of Security : Towards a Political Philosophy of Continental Thought », London, New York, Routledge, 1996.

- Dhillon, G. (1997), *Managing Information System Security*, 1e éd., Macmillan Press, 519 pages.

- Dhillon, G. (1999), « Managing and controlling computer misuse », *Information Management & Computer Security*, 7(4), 171-175.

- Dhillon, G. Syed, R., Pedron, C. (2016), « Interpreting information security culture: An organizational transformation case study », *Computers & Security*, Vol. 56 No. 2016, pp. 63–69.

- Dojkovski S., Warren, M., Lichtenstein, S., (2005), « Information Security Culture in Small and Medium Sized Enterprises: a Socio-cultural Framework », Proceedings of the 6th Australian Conference on Information Warfare and Security, 24-25 November 2005, Deakin University, Geelong, Australia

- Dojkovski, S., Lichtenstein, S. and Warren, M. (2006), *Challenges in fostering an information security culture in Australian small and medium sized enterprises*, 5th European conference on Information Warfare and Security, pp31-40.

- Dojkovski, S., Lichtenstein, S. and Warren, M. (2007), « Fostering Information Security Culture in Small and Medium Size Enterprises: An Interpretive Study in Australia », European Conference on Information Systems (ECIS), 2007.

- Drevon, E., Maurel, D., & Dufour, C. (2018). Veille stratégique et prise de décision : une revue de la littérature. *Documentation et Bibliothèques*, *64*(1), 28–34.

- Durand D., (2010), La systémique, 11ème édition, PUF, 102 pages.

- Dutta A., McCrohan K., (2002), « Management's role in information security in cyber economy », *California Management review*, Vol. 45 N°1, P67-87.

E

- Eisenhardt, K.M, (1991), « Better Stories and Better Constructs: The Case for Rigor and Comparative Logic », *Academy of Management Review*, Vol.16 n°3, pp. 620-627.

- Eisenhardt, K.M., 1(989), « Building Theories from Case Study Research », *Academy of Management Review*, 14(4), pp.532–550.

- Emery J.C., (1969), *Organizational planning and control system : Theory and technology*, Mac Millan, New York, USA.

- Evrard, Y., Pras B. et Roux, E. (2003), *Market – Etudes et recherches en marketing*, 3ème édition, Paris, Dunod.

- Eveloff S., (2005), « Take technology security serious-ly », *Pennsylvania CPA journal*, Vol 761, P.

F

- Fayolle, A (2017), *Création de valeur nouvelle et innovation* , Entrepreneuriat. Théories et pratiques, Applications pour apprendre à entreprendre, sous la direction de Fayolle Alain. Dunod, 2017, pp. 107-130.

- Fernandez-Toro, A. (2009), *Management de la sécurité de l'information : Implémentation ISO 27001 - Mise en place d'un SMSI et audit de certification*, Eyrolles, Paris, 2e édition.

- Filion, L.J. (1991), *Vision et relations : clefs du succès de l'entrepreneur* , Montréal, Les Éditions de l'Entreprise.

- Fishbein M., Ajzen, I., (1975), *Belief, Attitude, Intention and behaviour: An introduction to theory and research*, Addison-Wesley, Reading, MA, USA;

- Fitzgerald, T. (2007), *Building Management Commitment through Security Councils, or Security Council Critical Success Factors*, In H. F. Tipton (Ed.), Information Security Management Handbook (pp. 105-121). Hoboken: Auerbach Publications.

- Forcht K.A., Ayers W.C., (2000), « Developing a computer security policy for organizational use and implementation », *Journal of computer information systems*, winter 2000/2001, Vol.41,

- Fourcade C., Marchesnay M., (1997), *Gestion de la PME-PMI*, Nathan, Paris;

- Fourcade, C. (1991), *Petite entreprise et développement local*, Paris, *Eska.*

- Fourie, L. C. H. (2003). The management of Information Security- A South Africa case study. *South Africa Journal of Business Management 34*(2), 19-29.

- Freitag M. (1994), *Sicherheitskultur (Safety Culture) - ein brauchbares Konzept für Systemsicherheit und Arbeitssicherheit?*, in Psychologie der Arbeitssicherheit, Burkhardt F. and Winklmeier C., Eds. Heidelberg: Roland Asanger Verlag, 1994.

- Freyssinet-Dominjon, J. (1997), *Méthodes de recherche en sciences sociales*, Paris, Montchrestien, coll. AES, 1997.

- Friend M., Ridings-Pagliari L., (2000), « Establishing a safety culture: getting started », *Professional Safety*, May 2000, pp. 30-32;

- Furnell D .V. S.M., Jennex, M., Kritharas, I. (2004), Approaches to IT Security in Small and Medium Enterprises, Proceedings of the 2nd Australian Information Security Management Conference 2004, Perth, Australia.

- Furnell, S., Gennatou, M., Dowland, P. (2001), Promoting security awareness and training within small organizations, the 2nd AISM Workshop. N°2, pp. 52-57.

- Steven Furnell, Kerry-Lynn Thomson,(2009), « From culture to disobedience: Recognising the varying user acceptance of IT security », *Computer Fraud & Security*, Volume 2009, Issue 2, 2009, pp 5-10.

- Furnell, S., Emm, D., Papadaki, M. (2015), « The challenge of measuring cyber-dependent crimes », *Computer Fraud and Security*, October 2015: 5–12.

G

- Gadille, M. et D'Iribarne, A. (2000). « La diffusion d'Internet dans les PME, motifs d'adoption dans les réseaux et ressources mobilisées ». *Réseaux*, 18(104), 59-92.

- Gagnon, Y.C., (2012), *L'étude de cas comme méthode de recherche*, Presses de l'Université du Québec.

- Gattiker U.E., Kelley H., (1999), « Morality and computers : Attitudes and differences in moral judgments », *Information systems research*, Vol. 10 N°3, Septembre, pp. 233-254.

- Gaunt, N. (1998), « Installing an appropriate information security policy », *International Journal of Medical Informatics*, *49*(1), 131–134.

- Gaunt. (2000), « Practical Approaches to Creating Security Culture », *International Journal of Medical Informatics, 60*, 151-157.

- Gavard-Perret, M.L, Gotteland, D., Haon, C., Jolibert, A., (2018), *Méthodologie de la recherche en sciences de gestion : Réussir son mémoire ou sa thèse*. Pearson, 2018.

- Gavard-Perret, M.L., Helme-Guizon, A. (2008**)**. *Choisir parmi les techniques spécifiques d'analyse qualitative*, Dans M.L. Gavard-Perret, C. Haon, A. Jolibert (Éd.), *Méthodologie de la recherche. Réussir son mémoire ou sa thèse en sciences de gestion.* p. 247-280. Paris: Pearson Education.

- Genelot D. (1998), *Manager dans la complexité*, INSEP Editions.

- Gerber, M. & von Solms, R. (2005) « Management of risk in the information age », *Computers & Security*, 24(1):16-30

- Gervais, M. (1978), « Pour une théorie de l'organisation-PME », *Revue Française de Gestion*, n°15, p. 37-48.

- Ghernaouti-Helie, S. (2009), « An inclusive information society needs a global approach of information security », 2009 International Conference on Availability, Reliability and Security, IEEE Computer Society, pp. 658-662.

- Ghernaouti-Helie, S., Tashi, I. and Simms, D. (2010), « A multi-stage methodology for ensuring appropriate security culture and governance », 2010 International Conference on Availability, Reliability and Security, IEEE Computer Society, Krakow, pp. 353-359.

- Gilley A., Gilley J., McMillan H. (2009), « Organizational change: Motivation, communication, and leadership effectiveness », *Perform. Improv*. Q., vol. 21, no. 4, pp. 75–94, 2009.

- Giordano, Y. (2012), *Spécifier l'objet de la recherche*, in M.L. Gavard-Perret, D. Gotteland, C. Haon et A. Jolibert (Eds.), Méthodologie de la recherche en sciences de gestion, Réussir son mémoire ou sa thèse, 2ème édition, Montreuil : Pearson, 64-105.

- Girin J. (1986), L'objectivation des données subjectives. Éléments pour une théorie du dispositif dans la recherche interactive, Colloque ISEORFNEGE, « Qualité des informations scientifiques en gestion », p. 170-186.

- Girod-Séville M., Perret V. (1999), *Fondements épistémologiques de la recherche*, Méthodes de recherche en management, sous la direction de R.A.Thiétart, Edition Dunod, pp.13-33.

- Glaser B.G., Strauss A.L., (1967), *The Discovery of Grounded Theory : Strategies for Qualitative Research*, Chicago, Adline, 1967.

- Golhar, D.Y., Stamm, C.L. et Smith, W.L. (1990), « JiT implementation in small manufacturing firms», *Production and Inventory Management Journal*, 2e trimestre, p. 44-48.

- Gonik J., (1996), *Management de la sécurité des systèmes d'information* , Paris, Afnor;

- Goodhue D.L., Straub D.W., (1991), « Security concerns of systems users: a study of perceptions of the adequacy of security measures », *Information and Management* (20:1), January 1991, pp. 13-27;

- Goo, J., Yim, M.-S. and Kim, D.J. (2013), « A path way to successful management of individual intention to security compliance: a role of organizational security climate », 46th Hawaii International Conference on System Sciences (HICSS 2013), IEEE Computer Society, Wailea, HI, 7-10 January, pp. 2959-2968.

- Gottfredson M.R., Hirschi T.A., (1990), *General Theory of crime*, Stanford University press, Ca, USA.

- GREPME (1994), *Les PME: bilan et perspective* , Québec, Les Presses Inter Universitaires.

- Grover V., (1993), «Empirically derived model for the adoption of customer-based interorganizational systems », *Decision sciences*, Vol. 24, N°3, pp. 603-639.

- Guba, E.(1990), *The paradigm dialog*, Beverly Hills, CA: Sage.

- Guba, E. , Lincoln, Y., (1994), *Competing paradigms in qualitative research*, In N. K. Denzin & Y. S. Lincoln, eds. Handbook of qualitative research. London: Sage Publications, pp. 105–117.

- Guechtouli M. (2014)., « Management des activités de veille stratégique : entre une organisation formelle et informelle », *La Revue des Sciences de Gestion*, 2(2), 23-31.

- Guinier D., (1992), *Sécurité et qualité des systèmes d'information : approche systémique, la part de l'homme*, Paris, Masson.

- 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, pp. 297-310; Security, 24(1), 16-30.

- Guo K., Yufei Y., Archer N., Connelly C. (2011), « Understanding Non-Malicious Security Violations in the Workplace: A Composite Behavior Model », *Journal of Management Information Systems*, Vol. 28, n°2, p. 203-236.

H

- Haeussinger F., Kranz J., (2013), « Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior », In Proceedings of the International Conference on Information Systems ICIS 2013, Milan, Italy.

- Haidt J., Koller S.H., Dias M.G., (1993), « Affect culture, and morality, or is it wrong to eat your dog », *Journal of personality and social psychology*, N°65, pp. 613-618.

- Hallépée D. (2013), *La gouvernance des systèmes d'information : qualité et sécurité informatique*, Collection informatique, 2013.

- Hansche S., (2001), « Designing a security awareness program: part 1 », *Information systems security*, January/February, pp. 14-22.

- Harding, P. (2004), « Managing Change: A guide on how to manage change in an organisation », Sustainable Business Department, Government Office for the South West, 2004.

- Harrington S.J., (1996), « The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions », *MIS Quarterly*, September 1996, pp. 257-278.

- Harrison D. A., Mykytyn P. P., Riemenschneider C. K., (1997), « Executive Decisions about Adoption of Information Technology in Small Business: Theory and Empirical Tests », *Information Systems Research*, (8:2), pp. 171-195.

- Harnesk, D., Lindstrom, J. (2011), « Shaping security behaviour through discipline and agility implications for information security management », *Information Management & Computer Security*, Vol. 19 No. 4, pp. 262-276.

- Hassan N. H., Ismail Z., (2012), « A Conceptual Model for Investigating Factors Influencing Information Security Culture in Healthcare Environment », *Procedia - Social and Behavioral Sciences*, V 65, 2012, pp 1007-1012.

- Hassan, N. H., Ismail, Z. (2013), « Deriving the relationship between organizational culture and information security culture. *Vision 2020: Innovation, Development Sustainability, and Economic Growth »*, Proceedings of the 21st International Business Information Management Association Conference, IBIMA 2013, 2(December), 926–932.

- Hatchuel, A. (1994b), « Les savoirs de l'intervention en entreprise », *Entreprise et Histoire*, n° 7, pp. 59 à 75.

- Haydon, L. (2016), « People centric security - Transforming your enterprise security culture », McGraw-Hill Education, United States of America.

- Helme-Guizon, A., Gavard-Perret, M.L., (2004**)**, « L'analyse automatisée de données textuelles en marketing : comparaison de trois logiciels », *Décisions Marketing*, (36), 75-90.

- Helmich D.L., Brown W.B., (1972), «Successor type and organizational change in the corporate enterprise », *Administrative science quarterly*, (17), pp. 371-381;

- Helokunnas, T. et Kuusisto, R. (2003). « Information Security Culture in a Value Net », IEMC '03 Proceedings.

- Helokunnas, T., Iivonen, L., (2003), « Information security culture in small and medium size enterprises ». In e-Business Research Forum—eBRF 2003; Tampere University of Technology: Tampere, Finland, 2003.

- Herath, T., Rao, H.R. (2009b), « Protection motivation and deterrence: a framework for security policy compliance in organisations », *European Journal of Information Systems*, 18 (2), pp. 106– 125.

- Herath, T., Herath, H., Bremser, W.G. (2010), « Balanced Scorecard Implementation of Security Strategies: A Framework for IT Security Performance Management », *Information Systems Management*, Vol. 27, n° 1, p. 72-81.

- Hirschi T.A., (1969), « Causes of delinquency », University of California press, Berkeley, Ca, USA.

- Hofstede G (1998), « Identifying organizational subcultures: an empirical approach ». *Journal of Management Studies*, 35(1):1–12.

- Hofstede G., Bollinger D., (1987) « *les différences culturelles dans le management. Comment chaque pays gère-t-il ses hommes ?* », Les Editions d'organisations, 1987, 268 pages.

- Hofstede G, Neuijen B, Ohayv D, Sanders G (1990), « Measuring organizational cultures: a qualitative & quantitative study across twenty cases », *Administrative Science Quarterly*, Vol. 35, No. 2 (Jun., 1990), pp. 286-316.

- 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°4, p. 615-660.

- Huberman A.M., Miles M. B., (1991), *Analyse des données quantitatives : Recueil de nouvelles méthodes*, Bruxelles: De Boeck, 480 p;

- Hutchinson, D., Armitt, C., Edwards-Lear, D. (2014), « The application of an agile approach to it security risk management for SMES ». In Proceedings of the 12th Australian Information Security Management Conference, Perth, Australia, 1–3 December 2014.

- Hutchinson, D.; Warren, M., (2006), « e-Business Security Management for Australian Small SMEs—A Case Study ». In Proceedings of the 7th International We-B (Working for E-Business) Conference: e Business: How Far Have We Come? Orlando, Florida, 11–13 June 2006.

- Helokunnas, T., Iivonen, I., (2002), « Information security culture in small and medium size entreprises », Institute of Business Information Management, Tampere University of Technology, Finland.

- Henderson J., Venkatraman N., (1993), « Strategic alignment: Leveraging information technology for transforming organizations », *IBM systems journal* Vol 32, n°1.

- Herold R (2011) « Managing an information security and privacy awareness and training program ». Taylor and Francis, Boca Raton.

I

- IBM (2008), « Méthodologie de gestion du risque informatique pour les Directeurs des Systèmes d'Information : un levier exceptionnel de création de valeur et de croissance », Septembre 2008, p.14.

- Igalens. J., Roussel. O., (1998), *Méthodes de recherches en gestion des ressources humaines*, Paris, Economica, Recherches en gestion.

- Igbaria M., Zinatelli N., Cragg P., Cavaye A.L.M., (1997), « Personal computing acceptance factors in small firms: a structural equation model », *MIS Quarterly*, September 1997, pp. 279-305.

- Ikkou, L., Elouidani, A. (2016), « La gestion des risques des systèmes d'information dans les organismes publics au Maroc : quels bénéfices à la performance ? », *Revue Économie, Gestion et Société,* N°8 décembre 2016.

- Institut de la gouvernance des systèmes d'information (2005), « Place de la gouvernance des systèmes d'information dans la gouvernance générale de l'entreprise : équilibrer performance et conformité ». Institut de la gouvernance des systèmes d'information, AFAI, Cigref, 2005.

- International Nuclear Safety Advisory Group, (1986), « Summary Report on the Post-Accident Review Meeting on the Chernobyl accident », *Safety Series*, vol. 75-INSAG-1, 1986.

- International Standards Organization ISO/IEC TR 13335-1. (2004). *Information technology Security techniques Management of information and communications technology security Part 1: Concepts and models for information and communications technology security management.* ISO, 28 pages.

- ISACA (2008), *CISA review manuel 2008*, Information Systems Audit and Control Association, 580 pages.

- ISBS (2006), *Information Security Breaches Survey 2006*, Department of Trade and Industry, UK.

- Ismail O., Mourrain A., Cadiou C., (2019), *Vers une meilleure compréhension des comportements en matière de sécurité des systèmes d'information : Etude des PME Françaises et des PME Tunisiennes*, Intelligence économique et Intelligence Territoriale, Éditions Universitaires Européennes, Février 2019, ISBN 978-613-8-45511-0.

J

- Jaouen, A., Nakara, W. A. (2014). « Les systèmes d'information en microfirme : une approche par le bricolage organisationnel ». *Revue internationale P.M.E.*, 27 (3-4), 225–260.

- Jarvenpaa S.L., Ives B., (1991), « executive involvement and participation in the management of information technology », *MIS quarterly*, June 1991, pp 205-227.

- Jenkins P.H., (1997), « School delinquency and the school social bond », *Journal of research in crime and delinquency*, (34: 3), pp. 337-367.

- Julien P.A., Marchesnay M., (1996 et 1999), *L'entrepreneuriat*, Economica, Paris.

- Julien, P.A. (1994), *Les PME : bilan et perspectives*, Ed Economica, 352p, Paris.

- Julien, P.A., Marchesnay M. (1988), *La petite entreprise*, Editions Vuibert, 288p, Paris.

- Johnston A C., Warkentin M., Siponen M. (2015), « An enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric », *MIS Quarterly* Vol. 39, n°. 1, pp. 113-134.

- Johnsen, S.O., Hansen, C.W., Nordby, Y. and Dahl, M.B. (2006), « Measurement and improvement of information security culture », *Measurement and Control*, Vol. 39 No. 2, pp. 52-56.

- Johnson M. E., Goetz, E. (2007), «Embedding Information Security into the Organization », *IEEE Security & Privacy*,V5, 2007.

K

- Kahn R.L et Cannell C.F., (1957), The dynamics of interviewing. Theory, Technique, and cases, New York, Wiley & Sons, 1957.
- Kakar, S., Taylor F. W. (1970), *A Study in Personality and Innovation*, Cambridge, M.A., MIT Press, 1970.
- Karlsson, F. ; Astrom, J. ; Karlsson, M. (2015), « Information security culture – state-of-the-art review between 2000 and 2013 » *Information & Computer Security* Vol. 23 No. 3, 2015.
- Kaur, J., Mustafa, N. (2013), « Examining the Effects of Knowledge, Attitude and Behaviour on Information Security Awareness: A Case on SME », 3rd International Conference on Research and Innovation in Information Systems – 2013 (ICRIIS'13).
- Kefi H., Kalika M., (2004), E*valuation des systèmes d'information : une perspective organisationnelle*, Economica, Paris, 211 pages.
- Keller S., Powell A., Predmore C., Crawford M., (2005), « Information security threats and practices in small businesses », *Information systems management*, Spring, pp. 7-19.
- Kesh, S. & Ratnasingam, P. (2007), « A Knowledge Architecture for IT Security », *Communications of the ACM*, Vol. 50, n° 7, p. 103-108.
- Kim, S.H., Jang, S.Y., Yang, K.H., (2017), «Analysis of the Determinants of Software-as-a- Service Adoption in Small Businesses: Risks, Benefits, and Organizational and Environmental Factors», *Journal of Small Business Management*, Vol. 55, n°2, p. 303-325.
- Knapp, K. J., Marshall, T. E., Rainer, R. K., Morrow, D. W. (2004), «Top Ranked Information Security Issues ». In The 2004 International Information Systems Security Certification Consortium (ISC) 2 Survey Results., Alabama: Auburn University.
- Knapp, K. J., Marshall, T. E., Rainer, R. K., Ford, F. N. (2006), « Information Security: Management's Effect on Culture and Policy ». *Information and Computer Security*, 14(1), 24-36.
- Knapp, K.J., Marshall, T.E., Rainer, R.K. and Ford, F.N. (2007), "Information security: management's effect on culture and policy", Information Management & Computer Security, Vol. 14 No 1, pp. 24-36.

- Koenig, G. (1993), « Production de la connaissance et constitution des pratiques organisationnelles », *Revue de gestion des ressources humaines*, 9, 4-17.

- Koh, Ruighaver, A. B., Maynard, S. B., Ahmad, A. (2005), « Security Governance: Its Impact on Security Culture », Proceedings of the 3rd Australian Information Security Management Conference, Perth, Western Australia, 30th September 2005.

- Kolkowska, E. (2011), « Security subcultures in an organization-exploring value conflicts », 19th, European Conference on Information Systems (ECIS 2011), AIS Electronic Library, Helsinki, p. 237.

- Kokolakis S, Karyda M, Kiountouzis E (2005) « The insider threat to information systems and the effectiveness of ISO17799 ». *Computer Secur*ity 24(6):472–484.

- Kotulic A., Clark J.G., (2004), « Why there aren't more information security research studies », *Information and Management*, (41:5), pp 597-607.

- Kotter, J.P. (2006), « Leading change – why transformation efforts fail », *Harvard Business Review*, January 2007, pp. 1–10.

- Kraemer, S., Carayon, P. (2005), « Computer and information security culture: findings from two studies », *the Human Factors and Ergonomics Society Annual Meeting*, V. 49, No. 16, pp1483-1488.

- Kraemer S., Carayon P., (2006), « An adversarial viewpoint of human and organizational factors in computer and information security : Final report », Center for Quality and Productivity Improvement (CQPI), University of Wisconsin--Madison.

- Kraemer S., Carayon P., (2007), « Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists », *Applied Ergonomics*, Vol. 38, 16p;

- Krief, N., Zardet, V. (2013), « Analyse de données qualitatives et recherche-intervention », *Recherches en Sciences de Gestion*, 2(2), 211-237.

- Kroeber A. L., Kluckhohn C., (1952), *Culture : A Critical Review of Concepts and Definitions*. New York, Vintage Books, 1952.

- Kuusisto, T et Ilvonen, I (2003), «Information security culture in small and medium size entreprises », Frontiers of E-business research, Tampere University of Technology : University of Tampere, Finland, 2003.

- Kruger H.A., Kearney W. D., (2006), « A prototype for assessing information security awareness », *Computers & Security*, V 25, Issue 4, P 289-296.

- Kyobe M. (2008), « The impact of entrepreneur behaviours on the quality of ecommerce security: A comparison of urban and rural findings », *Journal of global information technology management*, Vol. 11, n°2, p. 58-79.

L

- Labodi, C., Michelberger, P., (2010), *Necessity or Challenge-Information Security for Small and Medium Enterprises*, Annals of the University of Petrosani, Economics, Vol. 10, n°3, p. 207-216.

- Lacey, D. (2010), « Understanding and transforming organizational security culture », *Information Management & Computer Security*, Vol. 18 No. 1, pp. 4–13.

- Lamère J.M., (1985), *La sécurité informatique : approche méthodologique* , Dunod, Paris,.

- Laplanche, J., Pontalis, j.B. (1967), *Vocabulaire de la psychanalyse*, , PUF, 1967, Paris.

- Lardeux L., (2014), Vulnérabilité, identification des risques et protection de l'enfance en danger , Observatoire Nationale de l'enfance en danger.

- Laudon K., Laudon J., Fimbel E., Costa S., (2010), « Management des systèmes d'information », Pearson, 551p.

- Le Blanc M., Kaspy N., (1998), « Trajectories of delinquency and problem behaviour: comparison of social and personal control characteristics of adjudicated boys on synchronous and non-synchronous paths », *Journal of Quantitative Criminology*, (14:2), pp. 181-214;

- Le Moigne J.L., (1973), *Les systèmes d'information dans les organisations*, Presses universitaires de France, Paris.
- Le Moigne J.-L. (1990), *Épistémologies constructivistes et sciences de l'organisation* , in Martinet (Ed.), Épistémologies et sciences de gestion, Economica, p. 81-140.

- Leclerc, Y., (1990), « De la sous-traitance au partenariat : le Japon, "modèle" de référence? », communication au colloque TETRA sur le thème "La PME : objet de recherche pertinent ?, 30-31 mai 1990, Lyon.

- Lee J., Lee Y., (2002), « A holistic model of computer abuse within organizations », *Information Management & Computer Security*, Vol. 10 N° 2, pp 57-63, MCB university Press.

- Lee Y., Kozar K.A., Larsen, K.R.T. (2003), « The technology acceptance model : past, present and future », *Communications of AIS*, Vol. 2003 N°12, pp. 752-780;

- 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.

- Lees, J.D., (1987), « Successful development of small business information systems ». *Journal of Systems Management*, 38(9), 32-39.

- Lemoigne, J-L (1993), « L'incongruité épistémologique des sciences de gestion », *Revue Française de Gestion*, n° 96, septembre-octobre 1993, p 123 à 135.

- Lesca H., Lesca E., Lesca N., Caron-Fasan ML. (2010), « Gestion de l'information : Qualité de l'information et performance de l'entreprise », Éditions EMS, 220p.

- Levy, M., Powell, P., Yetton, P. (2002). « The dynamics of SME information systems ». *Small Business Economics*, 19(4), 341-354.

- Lewin k. (1952), « Group decesions and social change », dans Swanson E., Newcom T. et Hartley E., Readings in Social Psychology, Holt Rinehart et Winston, New York, 1952.

- Lewin K. (1947), « Frontiers in Group Dynamics I », *Human Relations*, vol. 1, p. 5-41.

- Lewin K.,(1959), *Psychologie Dynamique les relations humaines*, Editions des Presses Universitaires de France, Collection Bibliothèque Scientifique Internationale.

- Lewin, K, (1967), *Psychologie dynamique : Les relations humaines*, Paris, PUF, 1959, 3ème édition, 1967, 296 pages.

- Lichtenstein, L., et Swatman, P. (2001). « Effective Management and Policy in e-Business Security », Paper presented at the 14th Bled Electronic Commerce Conference, Bled, Slovenia.

- Lim S.J, Chang S., Maynard, S., Ahmad, A., (2009), « Exploring the Relationship between Organizational Culture and Information Security Culture », *Proceedings of the 7th Australian Information Security Management Conference*, Perth, Western Australia, 1st to 3rd December 2009.

- Liu, M, (1983), *Approche socio-technique de l'organisation*, Paris, Editions d'organisation, 1983, 200 pages.

- Loch K., Carr H. H., M. Warkentin, W. (1992), « Threats to Information Systems: Today's Reality, Yesterday's Understanding », *MIS Quarterly*,V16, p 173-186.

- Longeon R., Archimbaud J.L., (1999), *Guide de la sécurité des systèmes d'information à l'usage des directeurs*, CNRS, Paris, 1999, 93 pages.

- Lopes, I., Oliveira, P. (2014), « Understanding Information Security Culture: A Survey in Small and Medium Sized Enterprises », *New Perspectives in Information Systems and Technologies*, Volume 1 pp 277-286.

M

- Mahe de Boislandelle, H., (1994), « Esquisse d'une théorisation de la GRH de la PME », communication au congrès de l'AGRH, Montpellier, p. 259-269.

- Malone, S.C. (1985), « Computerizing small business information systems ». *Journal of Small Business Management*, 23(2), 10-16.

- Mara, F. (2010), « Développement et Analyse des Critères de Vulnérabilité des populations Sahéliennes Face à la Variabilité du Climat: Le Cas de la Ressource en Eau dans la Vallée de la Sirba au Burkina Faso », Université du Québec à Montréal.

- Marchesnay, M. (1993), « PME, stratégie et recherche », *Revue Française de Gestion*, n°95, p. 70-76.

- Marchesnay, M. (a). (1982), *Pour un modèle d'hypofirme*, Entreprise et organisation, mélanges en l'honneur du professeur Aubert-Krier, Paris, Editions Economica, p. 71-91.

- Marchesnay, M. (b). (1982), « Is small so beautiful? », *Revue d'Economie Industrielle*, n°19, p. 110-114.

- Martinet B., Marty Y.M., (2001), *L'intelligence économique : comment donner de la valeur concurrentielle à l'information*, Editions d'organisation, Paris.

- Martins, A. (2002), « Information security culture », MCom dissertation, Rand Afrikaans University, Johannesburg.

- Martins, A. et Eloff, J.H.P. (2002). « Information security culture », *Security in the Information Society*, pp. 203 214.

- Martins, N., Da Veiga, A. (2015), « An Information security culture model validated with structural equation modelling ». Proceedings of the 9th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2015, Haisa, 11–21.

- Mason M., (2008), « Complexity Theory and the Philosophy of Education », *Educational Philosophy and Theory*, V 40, N1, pp 4618.

- Mathrani, S., Viehland, D. (2009). « Business benefits from enterprise systems implementation in small and medium-sized enterprises ». *Australasian Journal of Information Systems,* 16(1), 31-50.

- Mayer N., Humbert J.P., (2006), « La gestion des risques pour les systèmes d'information », MISC n°24 (Avril-Mai 2006), ISSN: 1631-9036.

- McCormac, A., Calic, D., Butavicius, M., Parsons, K., Zwaans, T., Pattinson, M. (2017), « A reliable measure of Information Security Awareness and the identification of bias in responses ». *Australasian Journal of Information Systems*, *21*, 1–12.

- McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., Pattinson, M. (2017). « Individual differences and Information Security Awareness », *Computers in Human Behavior*, *69*, 151–156.

- Mccoy, B., Stephens, G. and Stevens, K.J. (2009), « An investigation of the impact of corporate culture on employee information systems security behaviour », 20th Australasian Conference on Information Systems (ACIS 2009), AIS Electronic Library, Melbourne.

- Mehra, S., Inman, R.A. (1992), «Determining the critical elements of Just-in-Time implementation», *Decision Sciences*, vol. 23, n° 1, p. 160-174.

- Mijnhardt, F., Baars, T., et Spruit, M. (2016), «Organizational Characteristics Influencing SME Information Security Maturity», *Journal of Computer Information Systems*, Vol. 56, n°2, p. 106-115.

- Miles, M. B., Huberman, A. M. (2003). *Donner un sens : élaboration et vérification des conclusions. In Analyse des données qualitatives*, Méthodes en sciences humaines (2e éd), p. 437-518. Bruxelles: De Boeck.

- Miltgen, C. L., Peyrat-Guillard, D. (2014), « Cultural and generational influences on privacy concerns: A qualitative study in seven European countries », *European Journal of Information Systems*, *23*(2), 103–125.

- Mintzberg H., (1998), *Structure et dynamique des organisations*, Editions d'organisation, Paris.

- Mintzberg, H. (1989), « Mintzberg on Management : Inside Our Strange World of Organizations », New York, *The Free Press*.

- Moeller R., (2007), *COSO enterprise risk management: understanding the new integrated ERM framework*, Ed. Joh Wiley and Sons, 2007, ISBN 9780471741152.

- Moisand D., Garnier de Labareyre F., (2009), *CobiT Pour une meilleure gouvernance des systèmes d'information*, Eyrolles, Paris, 2009.

- Moisdon, J. C. (1984), « Recherche en gestion et intervention », *Revue Française de Gestion*, 47(48), 61-73.

- Moisdon J.-C. (2010), « L'évaluation du changement organisationnel par l'approche de la recherche-intervention. L'exemple des impacts de la T2A », *Revue Française des Affaires Sociales*, n°1-2, p. 213-226.

- Monnoyer M.C., (2003), *Le dirigeant confronté à la décision d'investissement en T.I.C*., in Boutary, TIC et PME : des usages aux stratégies, *l'Harmattan*, Paris.

- Moon Y. J., , Choi M., Armstrong D. J., (2018), « The impact of relational leadership and social alignment on information security system effectiveness in Korean governmental organizations », *International Journal of Information Management*, V 40,2018, P 54-66.

- Morin E., (1990), *Introduction à la pensée complexe*, Editions ESF, Collection communication et Complexité.

- Mourrain A., Leconte P. (2019), Comment la démarche projet de développement d'un Système d'Information est-elle impactée par le RGPD ? Cas d'une ETI du secteur de l'assurance, *24ème colloque de l'Association information et Management, Nantes, France.*

- Mucchielli, R. (1986). *Les méthodes qualitatives*. Paris : PUF

N

- Nance W.D., Straub D.W., (1988), « An investigation into the use and usefulness of security software in detecting computer abuse », proceedings of the ninth ICIS conference, DeGloss & Olson eds, Minneapolis, pp. 283-294.

- Nemati, H.R., Church, M. (2009), « A human centered framework for information security management: a healthcare perspective », Americas Conference on Information Systems 2009 (AMCIS 2009), AIS Electronic Library.

- Ngo, L., Zhou W., et Warren, M (2005)., « Understanding Transition towards Information Security Culture Change » », in Proceeding of the 3rd Australian Computer, Network & Information Forensics Conference, Edith Cowan University, School of Computer and Information Science, 2005, pp. 67–73.

- Njenga, K., Jordaan, P. (2016), «We Want to Do It Our Way: The Neutralisation Approach to Managing Information Systems Security by Small Businesses», *African Journal of Information Systems*, Vol. 8, n°1, p. 42-63.

- Nonaka, I. (1994). « A dynamic theory of organizational knowledge creation », *Organization Science*, Vol. 5, No. 1, pp 14-37.

- Nosworthy, J. (2000), «Implementing Information Security in the 21st Century - Do You Have the Balancing Factors », *Computers and Security*, 19(4): 337-347, 2000,

- Noteboom B., (1988), « The facts about small business and the real values of its 'life world », *American journal of economics and sociology* (47:3), July 1988, pp. 299-314.

O

- OECD (2002), *OECD Guidelines for the Security of Information Systems and Networks: Towords a culture of security*, 1037ème session, 25 juillet 2002.

- OECD., (2005), « The promotion of a culture of security for information systems and networks in OECD countries », www.oecd.org/internet/ieconomy/35884541.pdf.

- Okere I., van Niekerk J., Carroll M. (2012), « Assessing information security culture: A critical analysis of current approaches », in the proceedings of IEEE conference on Information Security for South Africa (ISSA), 2012, pp. 1 – 8.

- Orange Cyberdéfense (2019) : « Vulnérabilités : de quoi parle-t-on ? », https://orangecyberdefense.com/fr/insights/blog/gestion_des_vulnerabilites/vulnerabilites-de-quoi-parle-t-on/

P

- Parsons, K, M. Young, E. Butavicius, M, A. et McCormac, A. (2015), « The Influence of Organizational Information Security Culture on Information Security Decision Making », *Journal of Cognitive Engineering and Decision Making*, 2015, V 9, N 2, June 2015, pp. 117–129.
- Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., Jerram, C. (2014), « Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q) ». *Computers and Security*, *42*(September 2019), 165–176.

- Pattinson, M., Butavicius, M., Ciccarello, B., Lillie, M., Parsons, K., Calic, D., McCormac, A. (2018). « Adapting Cyber-Security Training to Your Employees », Proceedings of the Twelfth International Symposium on Human Aspects of Information Security \& Assurance (Haisa 2018), HAISA, 67–79.

- Pavlou P.A., Fygenson M., (2006), « Understanding and predicting electronic commerce adoption : and extension of the theory of planned behaviour", *MIS Quarterly*, Vol. 30 No. 1, pp. 115-143.

- Pavlou P.A., Fygenson M., (2006), « Understanding and predicting electronic commerce adoption : and extension of the theory of planned behaviour", *MIS Quarterly*, Vol. 30 No. 1, pp. 115-143;

- Pecqueur, B. (1989), *Un réseau ne se crée pas par défaut*, dans *M. Gault (éd.)*, Ville intermédiaire pour Europe, Paris.

- Pellemans, P. (1999), *Recherche qualitative en marketing : Perspective psychoscopique*, Bruxelles: De Boeck Université, 1999.

- Pérès A., Latour R, (2000), « Comportement ‘’sécuritaire’’ des utilisateurs des systèmes : observations empiriques », 21ème congrès de l’AFC, May 2000, France.

- Perks, S. (2010). « Problem-solving techniques of growing very small businesses ». *Journal of Enterprising Communities : People and places in the global economy*, 4(3), 220-233.

- Perreault P. (2012), *Le «ROI» de la Sécurité de l’information*, CISM, PCI QSA ,15 octobre 2012, p.11.

- Perret V., Séville M. (2007), *Fondements épistémologiques de la recherche*, in R.A. Thietart, Recherche en management, Dunod, p. 13-33.

- Peters, Thomas J., Richard H. Waterman (1982), *In Search of Excellence: Lessons from America's BestRun Companies*, New York: Harper & Row.

- Pettigrew, Andrew M. (1979) « On studying organizational cultures." *Administrative Science Ouarterly*, 24: 570-581.

- Piaget, J. (1967), *Logique et Connaissance scientifique*, Paris, Gallimard.

- Pipkin D., (2000), *Sécurité des systèmes d'information*, Paris, Campus Press, 391 pages.

- Pham, H. C., Pham, D. D., Brennan, L., Richardson, J. (2017). « Information security and people: A conundrum for compliance », *Australasian Journal of Information Systems*, V *21*, 1–16.

- Pritchard, S. (2010), «Navigating the Black Hole of Small Business Security», *Infosecurity*, Vol. 7, n°5, p. 18-21.

- Purtschert, R. (2001), *Marketing für Verbände und weitere Nonprofit-Organisationen*, Bern, Haupt.

R

- Ramachandran, S., Srinivasan, V. R., & Tim, G. (2008), « Information Security Cultures of Four Professions: A Comparative Study ». In Proceedings of the 41st Hawaii International Conference on System Sciences - 2008, Hawaii.

- Raymond L., (1990), « End-user computing in the small business context: foundations and directions for research », *Database*, (20:4), pp. 20-26;

- Raymond, L. (1985). « Organizational characteristics and mis success in the context of small business ». *MIS Quarterly*, 9(1), 37-52.

- Raymond, L. (2001). « Determinants of Web site implementation in small businesses ». *Internet Research*, 11(5), 411-424.

- Rees, J. (2010), «Information Security for Small and Medium-Sized Business», *Computer Fraud & Security*, Vol. 2010, n°9, p. 18-19.

- Reix R. (1984), *Traitement des données*, Foucher.

- Reix R. (2002), *Systèmes d'information et management des organisations*, Vuibert, 444 p.

- Reix R., Rowe F. (2002), *Faire de la recherche en système d'information*, collectif, Vuibert.

- Rest J.R., (1986), *Moral development: advances in research and theory*, Praeger publishers, New York, USA;

- Robbins S, Odendaal A, Roodt G. (2003), « Organisational behaviour –global and southern African perspectives ». Cape Town: Pearson Education South Africa; 2003.

- Robbins, S. P. (1989), *Organizational Behavior: Concepts, Controversies, and Applications*, (Fourth Edition ed.). New Jersey: Prentice Hall.

- Robinson S., Volonino L., (2004), *Principles and practices of information security*, Upper saddle river library, Pearson Prentice Hall.

- Rocher, G (1992), *La notion de culture*, Extraits du chapitre IV: "Culture, civilisation et idéologie", pp. 101-127. Montréal: Éditions Hurtubise HMH ltée, 1992, troisième édition.

- Rockart J.F., Crescenzi A.D., (1984), « Engaging top management in information technology », *Sloan management review*, Summer, pp. 3-16;

- Rockwell W.P., (1968), « MIS: a view from the top », *Dun's review* (92:4), October, pp 20-22.

- Romagni P., Wild V. (1998), *L'intelligence économique au service de l'entreprise*, éditions LES PRESSES DU MANAGEMENT, Paris, 1998, p.92.

- Ross, J. (2011), *Creating a Culture of Security*, ISACA, Rolling Meadows (2011).

- Royer C., Baribeau C., Duchesne A. (2009), « Les entretiens individuels dans la recherche en sciences sociales au Québec : où en sommes-nous ? Un panorama des usages », *Recherches Qualitatives*, Hors Série, n°7, p. 64-79.

- Rubin, H.J., Rubin, I.S. (1995) Qualitative Interviewing: *The Art of Hearing Data*. 2nd Edition, Sage Publications, London.

- Ruighaver, A. B., Maynard, S. & Chang, S. (2006). « Organizational Security Culture: Extending the End User Perspective », *Computers & Security*, vol. 26, no 1, p. 56-62.

- Ruighaver, A.B., Maynard, S.B. and Chang, S. (2007), « Organisational security culture: Extending the end-user perspective », *Computers and Security*, Vol. 26, No.1, pp56-62.

- Ravinchandran T., Lertwongsatien C., (2005), « Effect of information systems resources and capabilities on firm performance: A resource-based perspective », *Journal of Management Information Systems*, 21, 4 (Spring 2005), 237–276.

S

- Shahibi, M.S., Rashid, R.M., Fakeh, S.K.W., Dollah, W.A.K.W. and Ali, J. (2012), « Determining factors influencing information security culture among ICT librarians », *Journal of Theoretical and Applied Information Technology*, Vol. 37 No. 1, pp. 132-140.

- Saint-Jean M., Isus Barado S., Paris Manas G., Mace A., (2014) : « La recherche-intervention comme accompagnement du changement : le cas d'une formation de formateurs », *Les dossiers des sciences de l'éducation*, 31 | 2014, 31-48.

- Santos-Olmo A., Sánchez, L.E., Caballero I., Camacho, S., Fernandez-Medina, E. (2016), « The Importance of the Security Culture in SMEs as Regards the Correct Management of the Security of Their Assets », *Future Internet*, 2016, 8, 30.

- Savall H. (1975), *Enrichir le travail humain dans les entreprises et les organisation*, Editions Dunod, 213 pages.

- Savall H. (1979), *Reconstruire l'entreprise*, Dunod, (a).

- Savall H. (1979), *Stratégie socio-économique des entreprises*, Rapport au Commissariat Général du Plan, (b).

- Savall H.,(1989), *Enrichir le travail humain : L'évaluation économique*, Dunod, Paris, 1974, 1975 ; Economica, Paris, 5e édition, 1989.

- Savall H., Zardet V. (1996), « La dimension cognitive de la recherche intervention : la production de connaissances par interaction cognitive » *Revue Internationale de systémique*.Vol.10 n°1-2, p.161. pp157-189.

- Savall, H. et Zardet, V. (2004), *Recherche en Sciences de gestion : Approche Qualimétrique*, Economica.

- Schein E.H., (1984), « Coming to a New Awareness of Organizational Culture », *Sloan Management Review*, 25:2 (1984:Winter) p.3.

- Schein EH (1985), *Organizational culture and leadership*, San Francisco, Jossey-Bass, Publishers, 1985, 358 pages.

- Schein E. H. (1990), « Organizational Culture », *American Psychologist*, vol. 45, n° 2, 1990, pp. 109-119.

- Schein E. H. (1996), « Culture: The Missing Concept in Organization Studies », *Administrative Science Quarterly*, Vol. 41, No. 2, pp. 229-240.

- Schlienger T., Teufel, S. (2002), «Information Security Culture: The Socio-Cultural Dimension in Information Security Management », Security in the information society: visions and perspectives. IFIP TC11 International Conference on Information Security (Sec2002), Cairo, Egypt, Kluwer Academic Publishers.

- Schlienger T., Teufel, S. (2003), « Information security culture : From analysis to change », *South African Computer Journal, 31*, 46-52., 2003.

- Schultz E., (2004), « Security training and awareness : fitting a square peg in a round hole »,

- Sharkas, W. (1974). « The mini information system : an aid to small business survival ». *Journal of Small Business Management*, 12(3), 39-42.

- Shedden, P., Ahmad, A., & Ruighaver, A. B. (2006), « Risk Management Standard-the Perception of Ease of Use ». In Proceedings of the fifth annual security conference, Las Vegas, Nevada, USA.

- Sheptycki, J. (2004), « Organizational Pathologies in Police Intelligence Systems: Some Contributions to the Lexicon of Intelligence-Led Policing », European Journal of criminology, 2004, V1, I(3), p307-332.

- Sherif E., Furnell S., (2015) : « A Conceptual Model for Cultivating an Information Security Culture », *International Journal for Information Security Research* (IJISR), Volume 5, Issue 2, June 2015.
- Sherif, E., Furnell, S., Clarke, N. (2015), « An identification of variables influencing the establishment of information security culture », International Conference on Human Aspects of Information Security, Privacy, and Trust, pp436-448.
- Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F., and Downs, J. (2010), « Who Falls for Phishing?: A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions », in: Proceedings of the Sigchi Conference on Human Factors in Computing Systems. ACM, pp. 372-382.
- Silverzweig. Stan, and Robert F. Allen (1976), « Changing the corporate culture. », *Sloan Management Review*, Spring: 33-49.
- Silic, M., & Lowry, P. B. (2020), « Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance », *Journal of Management Information Systems*, *37*(1), 129–161.
- Simon D., (1997), *Contesting an Essential Concept : Reading the Dilemmas in Contemporary Security Discourse, in Critical Security Studies : concepts and cases*. UCL Press, London, 1997.
- Siponen, M.T. (2000), « A Conceptual Foundation for Organisational Information Security Awareness », *Information Management & Computer Security*, 8(1), 31-41.
- Soh C.P.P., Yap C.S., Raman K.S., (1992), « Impact of consultants on computerization success in small businesses », *Information and Management*, Vol. 22, pp. 309-319.
- Solomon S., (1986), « Small business USA: The role of small enterprises in sparking America's economy transformation », Crown publisher, N.Y., USA.
- Song J.H., (1982), « Diversification strategies and the experience of top executives of large firms », *Strategic management journal* (3), pp. 377-380.
- Spinellis D., Kokolakis S., Gritzalis S., (1999), « Security requirements, risks and recommendations for small enterprise and home-office environments », *Information Management and Computer Security*, Vol.7 N°3, pp. 121-128.
- Sproul L., Kiesler S., (1991), *Connections: New Ways of Working in the Networked Organization*, MIT press, Boston, USA.
- Stake, R.E., (2005), *Qualitative Case Studies*. In N. K. Denzin & Y. S. Lincoln, eds. Handbook of Qualitative Research. Thousand Oaks: Sage Publications, pp. 443–466.

- Stevens J.M., Beyer J.M., Trice M.H., (1978), « Assessing personal role and organizational predictors of managerial commitment », *Academy of management journal* (21), pp. 380-396.

- Štemberger, M. I., Manfreda, A., & Kovačič, A. (2011), « Acheng top management support with business knowledge and role of IT/IS personnel », *International Journal of Information Management*, *31*(5), 428–436.

- Straub D.W., Welke R., (1998), « Coping with systems risk: security planning models for management decision making », *MIS quarterly*, December, pp. 441-469.

T

- Tang, M., Li, M., Zhang, T. (2016), « The impacts of organizational culture on information security culture: a case study », *Information Technology and Management* (2016) 17:179–186.

- Tarimo, C. (2006), *ICT Security Readiness Chechlist for Developing Coutries: A Social-Technical Approach*, Unpublished PhD Thesis, Stockolm University, Royal Institute of Technology.

- Taylor S., Todd P. A., (1995a), « Assessing IT Usage: The Role of Prior Experience », *MIS Quarterly*, (19:2), pp. 561-570.

- Taylor, F.W. (1911), *The Principles of Scientific Management*. New-York: Harper and Brothers.

- Pritchard S., Todd P. A., (1995b), « Understanding Information Technology Usage: A Test of Competing Models, », *Information Systems Research*, (6:4), pp. 144-176;

- Taylor M.; Murphy, A. (2004), « SMEs and eBusiness ». *Journal of small business and enterprise*, 2004, 11, 280–289.

- Tessem H.M., Skaaraas, K.R. (2005), « Creating a security culture », *Information Society and Security*, p15.

- Theys J. (2003), « La Gouvernance, entre innovation et impuissance : le cas de l'environnement », Développement durable et territoires, Dossier n° 2 : Gouvernance locale et développement durable.

- Thietart R.A. (dir.) et al. (2014), *Méthodes de recherche en management*, 4ème édition, Management Sup, Dunod, 656 p.

- Thompson R. L., Higgins, C. A., Howell, J. M., (1991), « Personal Computing: Toward a Conceptual Model of Utilization », *MIS Quarterly*, (15:1), pp. 124-143;

- Thomson, K., von Solms, R. (2005), « Information Security Obedience: A Definition », *Computers & Security*, 24(1), 69-75.

- Thomson, KL ; Von Solms, R ; Louw, L (2006), « Cultivating an organizational information security culture », *Computer Fraud & Security*, octobre 2006, p 7-11.

- Thong J.Y.L, Yap C.S., Raman K.S., (1996), « Top management support, external expertise and information systems implementation in small businesses », *Information systems research*, Vol.7, N° 2, pp 248-267.

- Tolah, A., Furnell, S. M., Papadaki, M. (2017), « A Comprehensive Framework for Cultivating and Assessing Information Security Culture », The Eleventh International Symposium on Human Aspects of Information Security & Assurance *(HAISA), HAISA 2017*, 52–64.

- Torrès O., (1998), *PME : de nouvelles approches*, Economica, Paris;

- Torrès, O. (1998), « Vingt-Cinq Ans De Recherche En Discipline Entre Courants Et Contre-Courants. *PME : De Nouvelles Approches*, 187.

- Trauth, E. M., & Jessup, L. M. (2000), « Understanding Computer-Mediated Discussions: Positivist and Interpretive Analyses of Group Support System Use ». *MIS Quarterly*, 24, 43-79.

- Triandis H. C., (1977), *Interpersonal Behavior*, Brooke/Cole, Monterey, USA;

- Tylor, Edward B., (1871), Primitive Culture : Researches into the Development of Mythology, Philosophy, Religion, Art, and Custom. London: John Murray.

V

- Vallerand R. J., (1997), *Toward a Hierarchical Model of Intrinsic and Extrinsic Motivation*, in Advances in Experimental Social Psychology (29), M. Zanna (ed.), Academic Press, New York, pp. 271-360.
- van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human Computer Studies*, *123*(November 2018), 29–39.

- Van de Ven, A.H., et M.S. Poole, (2002), *Field Research Methods*, in J.A.C. Baum (Ed.), Companion to Organizations, Oxford : Blackwell, 867-888.

- Van Niekerk J.F., Von Solms R., (2010), « Information security culture: A management perspective », *computers & security* 29 (2010) 476 – 486.

- Van Niekerk, J., Von Solms, R. (2005), « A holistic framework for the fostering of an information security sub-culture in organizations », in Venter, H.S., Eloff, J.H., Labuschagne.

- Van Niekerk, J., & Von Solms, R. (2006). Understanding Information Security Culture: A Conceptual Framework. *Proceedings of ISSA 2006*, 1–10.

- Venkatesh V., Davis F. D., (2000), « A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies », *Management Science*, (45:2), pp. 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, pp. 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* (79:1), pp. 1-28;

- Venter, H.S. et Eloff J.H.P (2003), « A taxonomy for information security technologies » *Computers & Security* 22(4):299-307 · May 2003.

- Vermeulen C., Von Solms R., (2002), « The information security management toolbox: Taking the pain out of security management », *Information management & Computer Security*, pp 119-125.

- Von B.L (1993), *Théorie générale des systèmes*, 1993, Nouvelle édition, Edition Dunod, 308 pages.

- Von Solms R., Van de Haar, (2000), « From Trusted Information Security Controls to a Trusted Information Security Environment », Actes de la 16th Annual Working Conference on Information Security, IFIP, Août, Beijing, Chine, contribution n°4/52;

- Von Solms, S. (2000), « Information Security- The Third Wave? », *Computer & Security*, 19, 615-620.

- Vroom, C., & von Solms, R. (2004). « Towards Information Security Behavioral Compliance », *Computers & Security*, 23(3), 191-198.

- Voynnet F. C. (2006), « Le codage à visée théorique », *Recherche et Applications en Marketing, 21* (4), 61-78.

W

- Wacheux F., (1996), *Méthodes qualitatives et recherche en gestion*, Economica, Paris.
- Waever O. , (1997), « Concepts of Security », Institute of Political Sciences, University of Copenhagen, 1997.
- Wang, J. (2015), « Research article insider threats in a financial institution : Analysis attack proneness of information systems applications », *MIS Quarterly*, V. 39, No. 1 (March 2015), pp. 91-112.
- Wang, J., Li, Y., Rao, H. R. (2017), « Coping responses in phishing detection : An investigation of antecedents and consequences », *Information Systems Research*, *28*(2).
- Walsham G., (1993), «Interpreting information systems in organizations», Wiley & Sons, Chichester.
- Walster R., Walster G., Berschied E., (1978), *Equity: Theory and research*, Allyn and Bacon, Needham heights, USA.
- Warren M.J. (2003), « Australia ‘s Agenda for E-Security Education and Research ». In: Irvine C., Armstrong H. (eds) Security Education and Critical Infrastructures. WISE 2003. IFIP Advances in Information and Communication Technology, vol 125. Springer, New York, NY.
- Weill P., Ross J., (2004), *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*, Harvard Business School Press, Boston, 2004.
- Westrum, R. (1993), « Cultures with Requisite Imagination ». In J.Wise, P.Stager & J.Hopkin (Eds.) Verification and Validation in Complex Man-Machine Systems. Springer, New York pp 401-416.
- Welsh, J.A et White J.F. (1981), « A small business is not a little big business », Harvard Business Review, Vol 59, n°4, p. 18-32.
- Williams, P.A.H. (2008), « In a ‘trusting’ environment, everyone is responsible for information security », *Information Security Technical Report*, Vol. 13 No. 4, pp. 207-215.
- Williams, P.A. (2009), « What Does Security Culture Look Like For Small Organizations? », Proceedings of the 7th Australian Information Security Management Conference, 2009.
- Winston, R. Heiko L. (1990), «Just-in-Time and small business evolution», *Entrepreneurship : Theory and Practice*, été, p. 51-64.

- Wilderom C. P. M., Van den Berg P. T., Wiersma U. J. (2012), « A longitudinal study of the effects of charismatic leadership and organizational culture on objective and perceived corporate performance », *The Leadership Quarterly*, V 23, Issue 5, pp 835-848.
- Willison R., Warkentin M., (2013), « Beyond Deterrence: An Expanded View of Employee Computer Abuse », *MIS Quarterly*, 37(1):1-20.

Y

- Yap C.S., (1989), « Issues in managing information technology », *Journal of operational research society*, 40:7, UK, pp 649-658.
- Yin, R.K., (1994), *Case study research: Design and methods Second*., Sage Publications.
- Yin, R.K., (2003), *Applications of Case Study Research (Applied Social Research Methods)*, Sage Publications, Inc.
- Yoo, C. W., Sanders, G. L., Cerveny, R. P. (2018), « Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance ». *Decision Support Systems*, *108*(March), 107–118.

Z

- Zwingelstein G., (1996), *Diagnostic des défaillances – Théorie et pratique pour les systèmes industriels*, 1996, Hermes, 666 pages.

Table des matières

Liste des annexes

Annexe 1 : Charte de la sécurité des systèmes d'information (Dans le cadre de l'intervention)

Charte de la sécurité des systèmes d'information utilisateur

Classification	PUBLIC – INTERNE – CONFIDENTIEL ☐ ☐ ☐		
Crée par	Olfa ISMAIL		
Propriétaire			
Validation			
Diffusion	INTERNE		
Version	Numéro de version	Date	Détails des modifications

*Ce document devra comporter votre signature ainsi que la date sur la dernière page.

Sommaire

1. Préambule

Cette Charte décrit les bonnes pratiques comportementales devant être connues et appliquées afin d'assurer les conditions d'un usage correct et sécurisé du Système d'Information. Celui-ci se compose de l'ensemble des moyens humains, techniques et organisationnels permettant, en support à l'activité, de créer, de conserver, d'échanger, de communiquer et de partager des informations entre les acteurs internes et externes quelle que soit la forme sous laquelle elles sont exploitées (électronique, imprimée, manuscrite, vocale, image, etc.).

Cette charte a pour objet :

- De faire prendre conscience des enjeux de la sécurité et de responsabiliser chaque Utilisateur, individuellement

- De mettre en évidence la nécessité, pour la sécurité de tous, que chacun adopte un comportement loyal, responsable et vigilant et respecte les principes et recommandations édictés par …….. en matière d'utilisation du Système d'Information

- De préciser les droits, les devoirs et les responsabilités de chacun en accord avec la législation en vigueur

- D'informer chaque Utilisateur des moyens mis en œuvre pour le contrôle de l'usage des Ressources du Système d'Information.

Les principes énoncés ne sont pas exclusifs de l'application des lois, de l'ensemble de la réglementation interne du Groupe et des règles de courtoisie et de respect d'autrui.

2. Application

La présente Charte s'applique à l'ensemble des Utilisateurs du Système d'Information, en ce compris les collaborateurs, quel que soit leur statut, et plus généralement à l'ensemble des personnes intervenant pour le compte de ……. et ayant accès aux Ressources de son Système d'Information. Elle est diffusée individuellement et s'impose à chacun.

Le non-respect de cette charte peut conduire, à la discrétion de ……., à une restriction temporaire ou une révocation définitive des droits d'accès au Système d'Information; il peut également entraîner des sanctions disciplinaires, dans le respect des procédures applicables, sans préjuger des éventuelles poursuites judiciaires qui pourraient être envisagées.

3. Règles générales d'utilisation

Chaque Utilisateur est responsable à titre personnel d'une utilisation du Système d'Information conforme aux lois et règlements en vigueur.

L'utilisateur DOIT	L'utilisateur NE DOIT PAS
-Respecter les règles relatives à la confidentialité et à la protection des données à caractère personnel	- Chercher à porter atteinte directement ou indirectement aux droits des personnes ainsi qu'à leur vie privée ou au droit des biens
- Respecter les règles de protection du droit d'auteur en ne se rendant pas coupable de contrefaçon	- Détourner à son profit ou à celui d'un tiers tout ou partie du Système d'Information auquel il a accès
	- Surveiller les autres Utilisateurs sauf autorisation expresse donnée par la Direction Générale.

4. Accès aux ressources

L'accès aux Ressources du Système d'Information n'est possible que dans le cadre de l'activité professionnelle des Utilisateurs, défini par leur fonction, et dans les limites des délégations qui leur sont accordées.

A cet égard, toutes les informations, données ou communications électroniques émises, reçues ou stockées au moyen de ces ressources, ainsi que tous les documents et fichiers enregistrés par l'Utilisateur, sont présumés avoir un caractère professionnel.

L'accès à certaines Ressources du Système d'Information est soumis à l'usage d'un code d'accès strictement personnel. Son utilisation engage la responsabilité du titulaire. Il ne peut en aucune manière être communiqué à un tiers, même temporairement.

Les droits d'accès aux Ressources du Système d'Information nécessitant un mot de passe peuvent être suspendus ou révoqués à tout instant par ……., notamment en cas de suspension momentanée ou d'arrêt définitif de l'activité professionnelle.

5. Sécurité informatique

5.1 Principe général de responsabilité et obligation de prudence

L'utilisateur est responsable des ressources informatiques qui lui sont confiées dans le cadre de ses missions, et doit concourir à leur protection, notamment en faisant preuve de prudence. L'utilisateur doit s'assurer d'utiliser les ressources informatiques mises à sa disposition de manière raisonnable, conformément à ses missions.

5.2 Obligation générale de confidentialité

L'utilisateur s'engage à préserver la confidentialité des informations, et en particulier des données personnelles, traitées sur le SI de l'entreprise. IL s'engage à prendre toutes les précautions utiles pour éviter que ne soient divulguées de son fait, ou du fait de personnes dont il a la responsabilité, ces informations confidentielles.

5.3 Mot de passe

L'accès aux SI ou aux ressources informatiques mises à disposition est protégé par mot de passe individuel. Ce mot de passe doit être gardé confidentiel par l'utilisateur afin de permettre le contrôle de l'activité de chacun. Le mot de passe doit être mémorisé et ne doit pas être écrit sous quelque forme que ce soit. Il ne doit pas être transmis ou confié à un tiers

ou être rendu accessible. Le login et le mot de passe doivent être saisis lors de chaque accès au système d'information.

Le mot de passe doit se conformer à la politique de mot de passe édictée conformément aux prescriptions de la CNIL relativement à la protection des données personnelles et notamment:

-être composé de plus de 12 caractères,

-ces caractères doivent être une combinaison de caractères alphanumériques de chiffres,

-de majuscules,

-de minuscules,

-et de caractères spéciaux.

5.4 Verrouillage de sa session

L'utilisateur doit veiller à verrouiller sa session dès lors qu'il quitte son poste de travail.

5.5 Installation de logiciels

L'utilisateur ne doit pas installer, copier, modifier ou détruire de logiciels sur son poste informatique sans l'accord du service informatique en raison notamment du risque de virus informatiques.

5.6 Copie de données informatiques

L'utilisateur doit respecter les procédures définies par l'organisme afin d'encadrer les opérations de copie de données sur des supports amovibles, notamment en obtenant l'accord préalable du supérieur hiérarchique et en respectant les règles de sécurité, afin d'éviter la perte de données (ex : vol de clé usb, perte d'un ordinateur portable contenant d'importantes quantités d'informations confidentielles…).

6. Accès à internet et messagerie

L'accès à l'Internet est autorisé au travers du SI, toutefois, pour des raisons de sécurité l'accès à certains sites peut être limité.
La dépendance croissante des Utilisateurs du Système d'Information à l'égard des services offerts par Internet (sites web, forums, blogs, etc.) et par la messagerie met en évidence de nouveaux risques auxquels il faut être particulièrement attentif.

Tout utilisateur doit prévoir un message d'absence en indiquant à ses correspondants l'identité et les coordonnées des personnes à contacter.

Conditions vis-à-vis du droit au secret des correspondances :

Les courriers ayant un objet personnel doivent demeurer limités dans leur nombre et doivent être classés dans un répertoire dénommé « privé / personnel / perso » de la boîte de réception.

L'utilisateur doit inviter ses correspondants à mentionner le caractère « privé / personnel / perso » du message dans son objet.

De manière préventive, ……. peut mettre en œuvre un certain nombre de dispositifs de filtrage, notamment à l'égard de sites Internet dont le contenu peut être contraire à l'ordre public ou aux bonnes mœurs.

7. Sanctions

Les manquements aux règles édictées par la présente charte peuvent engager la responsabilité de l'utilisateur et entraîner des sanctions à son encontre (limitation d'usage du SI, sanctions disciplinaires).

8. Entrée en vigueur

La présente charte est ajoutée en annexe du règlement intérieur et communiquée individuellement à chaque employé. Elle entre en vigueur au :

9. Signature de la charte

Après lecture des pages composant cette charte informatique utilisateur, vous déclarez avoir pris connaissance de l'ensemble des obligations que …….. attend de votre part. De fait, vous vous engagez à respecter l'ensemble des éléments notifiés dans l'ensemble de ce document.

Prénom et Nom :

Date :

Signature :

Annexe 2 : Questionnaire avant intervention

Sécurité des systèmes d'information (Avant intervention)

Le système d'information est un ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information.

*Obligatoire

1. Vous êtes *

Une seule réponse possible.

- ◯ femme
- ◯ homme

2. Votre âge *

Une seule réponse possible.

- ◯ 18-24 ans
- ◯ 25-34 ans
- ◯ 35-44 ans
- ◯ 45-54 ans
- ◯ 55-64 ans

3. Votre poste *

Une seule réponse possible.

- ◯ Lié à des informations sensibles (RH, comptabilité etc)
- ◯ Non lié à des informations sensibles

4. Je sais qu'est-ce qu'un incident de sécurité *

Une seule réponse possible.

- ◯ Pas d'accord
- ◯ D'accord

5. Je suis autorisé à partager mon mot de passe avec des collègues *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Je ne sais pas
- ◯ D'accord
- ◯ Tout à fait d'accord

6. C'est une mauvaise idée de partager mes mots de passe professionnels, même si un collègue le demande *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Je ne sais pas
- ◯ D'accord
- ◯ Tout à fait d'accord

7. Je partage mon mot de passe avec mes collègues *

Une seule réponse possible.

- ◯ Pas d'accord
- ◯ D'accord

8. Un mélange de lettres, de chiffres et de symboles est nécessaire pour les mots de passe professionnels *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Je ne sais pas
- ◯ D'accord
- ◯ Tout à fait d'accord

9. C'est sans danger d'avoir un mot de passe avec juste des lettres *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Je ne sais pas
- ◯ D'accord
- ◯ Tout à fait d'accord

10. J'utilise une combinaison de lettres, de chiffres et de symboles dans mes mots de passe professionnels *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Je ne sais pas
- ◯ D'accord
- ◯ Tout à fait d'accord

11. Je suis autorisé à cliquer sur n'importe quel lien dans les e-mails de personnes que je connais *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Je ne sais pas
- ◯ D'accord
- ◯ Tout à fait d'accord

12. Il est toujours sans danger de cliquer sur des liens dans les e-mails de personnes que je connais *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Je ne sais pas
- ◯ D'accord
- ◯ Tout à fait d'accord

13. Je ne clique pas toujours sur les liens dans les e-mails simplement parce qu'ils proviennent de quelqu'un que je connais *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Je ne sais pas
- ◯ D'accord
- ◯ Tout à fait d'accord

14. Je suis autorisé à entrer des informations sur n'importe quel site Web si cela m'aide à faire mon travail *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Je ne sais pas
- ◯ D'accord
- ◯ Tout à fait d'accord

15. Si cela m'aide à faire mon travail, peu importe les informations que je mets sur un site Web *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Je ne sais pas
- ◯ D'accord
- ◯ Tout à fait d'accord

16. Je vérifie la sécurité du site Web avant de saisir des informations *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Je ne sais pas
- ◯ D'accord
- ◯ Tout à fait d'accord

17. Je peux publier ce que je veux concernant mon travail sur les réseaux sociaux *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Je ne sais pas
- ◯ D'accord
- ◯ Tout à fait d'accord

18. Il est risqué de publier certaines informations concernant mon travail sur les réseaux sociaux *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Je ne sais pas
- ◯ D'accord
- ◯ Tout à fait d'accord

19. Je publie ce que je veux concernant mon travail sur les réseaux sociaux *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Je ne sais pas
- ◯ D'accord
- ◯ Tout à fait d'accord

20. Lorsque je travaille sur des fichiers sensibles, je dois m'assurer que les autres ne peuvent pas voir l'écran de mon ordinateur *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Je ne sais pas
- ◯ D'accord
- ◯ Tout à fait d'accord

21. Il est risqué d'accéder à des fichiers de travail sensibles sur un ordinateur si quelqu'un peut voir mon écran *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Je ne sais pas
- ◯ D'accord
- ◯ Tout à fait d'accord

22. Je vérifie que les autres ne peuvent pas voir l'écran de mon ordinateur si je travaille sur un document sensible *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Je ne sais pas
- ◯ D'accord
- ◯ Tout à fait d'accord

23. Les impressions sensibles peuvent être traitées de la même manière que les impressions non sensibles *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Je ne sais pas
- ◯ D'accord
- ◯ Tout à fait d'accord

24. L'élimination des impressions sensibles en les mettant dans la poubelle est sans danger *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Je ne sais pas
- ◯ D'accord
- ◯ Tout à fait d'accord

25. Lorsque des impressions sensibles doivent être éliminées, je m'assure qu'elles sont déchiquetées ou détruites *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Je ne sais pas
- ◯ D'accord
- ◯ Tout à fait d'accord

26. Si je trouve une clé USB dans un lieu public, je ne devrais pas la brancher sur mon ordinateur de travail *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Je ne sais pas
- ◯ D'accord
- ◯ Tout à fait d'accord

27. Si je trouve une clé USB dans un lieu public, rien de grave ne peut se produire si je la branche sur mon ordinateur de travail *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Je ne sais pas
- ◯ D'accord
- ◯ Tout à fait d'accord

28. Je ne brancherais pas une clé USB trouvée dans un lieu public sur mon ordinateur de travail *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Je ne sais pas
- ◯ D'accord
- ◯ Tout à fait d'accord

29. Si je vois quelqu'un agir de manière suspecte sur mon lieu de travail, je devrais le signaler *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Je ne sais pas
- ◯ D'accord
- ◯ Tout à fait d'accord

30. Si j'ignore quelqu'un qui agit de manière suspecte sur mon lieu de travail, rien de mal ne peut arriver *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Je ne sais pas
- ◯ D'accord
- ◯ Tout à fait d'accord

31. Si je voyais quelqu'un agir de manière suspecte sur mon lieu de travail, je ferais quelque chose à ce sujet *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Je ne sais pas
- ◯ D'accord
- ◯ Tout à fait d'accord

32. Je sauvegarde régulièrement tous les fichiers et les données (sur le serveur, sur l'ordinateur, dans le drive etc.) *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Je ne sais pas
- ◯ D'accord
- ◯ Tout à fait d'accord

33. Je sais qu'elles sont mes responsabilités en matière de sécurité de l'information *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Je ne sais pas
- ◯ D'accord
- ◯ Tout à fait d'accord

34. Je crois avoir une responsabilité concernant la protection du système d'information de l'entreprise (par exemple, les informations et les ressources informatiques). *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Je ne sais pas
- ◯ D'accord
- ◯ Tout à fait d'accord

35. La sécurité des systèmes d'information est avant tout une question technique (elle concerne principalement la division informatique) *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Je ne sais pas
- ◯ D'accord
- ◯ Tout à fait d'accord

36. Je connais les aspects de sécurité des informations liés à ma fonction professionnelle (par exemple, comment choisir un mot de passe ou gérer des informations confidentielles) *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Je ne sais pas
- ◯ D'accord
- ◯ Tout à fait d'accord

37. Je crois que les exigences de sécurité des systèmes d'information devraient être intégrées à mes tâches quotidiennes. *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Je ne sais pas
- ◯ D'accord
- ◯ Tout à fait d'accord

38. Je pense qu'il est nécessaire d'engager les gens dans la sécurité des systèmes d'information *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Je ne sais pas
- ◯ D'accord
- ◯ Tout à fait d'accord

39. Mes collègues font preuve d'engagement envers la sécurité des systèmes d'information *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Je ne sais pas
- ◯ D'accord
- ◯ Tout à fait d'accord

40. Je pense que l'entreprise met en œuvre des mesures de sécurité des systèmes d'information *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Je ne sais pas
- ◯ D'accord
- ◯ Tout à fait d'accord

41. La sécurité des systèmes d'information est perçue comme importante par le dirigeant *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Je ne sais pas
- ◯ D'accord
- ◯ Tout à fait d'accord

42. J'ai lu la charte de sécurité des systèmes d'information *

Une seule réponse possible.

- ◯ Pas d'accord
- ◯ D'accord

43. J'ai participé à une formation et/ou j'ai eu des cours (en ligne par exemple) lié à la sécurité des systèmes d'information *

Une seule réponse possible.

- ◯ Pas d'accord
- ◯ D'accord

Annexe 3 : brochure de sensibilisation à la sécurité des SI

Annexe 4 : Affiche de sensibilisation aux sauvegardes de données

Annexe 5 : Questionnaire après intervention

Sécurité des systèmes d'information (Après intervention)

*Obligatoire

1. Vous êtes *

Une seule réponse possible.

- ◯ femme
- ◯ homme

2. Votre âge *

Une seule réponse possible.

- ◯ 18-24 ans
- ◯ 25-34 ans
- ◯ 35-44 ans
- ◯ 45-54 ans
- ◯ 55-64 ans

3. Votre poste *

Une seule réponse possible.

- ◯ Lié à des informations sensibles (RH, comptabilité etc)
- ◯ Non lié à des informations sensibles

4. Je sais qu'est-ce qu'un incident de sécurité *

Une seule réponse possible.

- ◯ Pas d'accord
- ◯ D'accord

5. Je suis autorisé à partager mon mot de passe avec des collègues *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Ni d'accord ni en désaccord
- ◯ D'accord
- ◯ Tout à fait d'accord

6. C'est une mauvaise idée de partager mes mots de passe professionnels, même si un collègue le demande *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Ni d'accord ni en désaccord
- ◯ D'accord
- ◯ Tout à fait d'accord

7. Je partage mon mot de passe avec mes collègues *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Ni d'accord ni en désaccord
- ◯ D'accord
- ◯ Tout à fait d'accord

8. Un mélange de lettres, de chiffres et de symboles est nécessaire pour les mots de passe professionnels *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Ni d'accord ni en désaccord
- ◯ D'accord
- ◯ Tout à fait d'accord

9. C'est sans danger d'avoir un mot de passe avec juste des lettres *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Ni d'accord ni en désaccord
- ◯ D'accord
- ◯ Tout à fait d'accord

10. J'utilise une combinaison de lettres, de chiffres et de symboles dans mes mots de passe professionnels *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Ni d'accord ni en désaccord
- ◯ D'accord
- ◯ Tout à fait d'accord

11. Je suis autorisé à cliquer sur n'importe quel lien dans les e-mails de personnes que je connais *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Ni d'accord ni en désaccord
- ◯ D'accord
- ◯ Tout à fait d'accord

12. Je ne clique pas toujours sur les liens dans les e-mails simplement parce qu'ils proviennent de quelqu'un que je connais *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Ni d'accord ni en désaccord
- ◯ D'accord
- ◯ Tout à fait d'accord

13. Je suis autorisé à entrer des informations sur n'importe quel site Web si cela m'aide à faire mon travail *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Ni d'accord ni en désaccord
- ◯ D'accord
- ◯ Tout à fait d'accord

14. Je vérifie la sécurité du site Web avant de saisir des informations *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Ni d'accord ni en désaccord
- ◯ D'accord
- ◯ Tout à fait d'accord

15. Les impressions sensibles peuvent être traitées de la même manière que les impressions non sensibles *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Ni d'accord ni en désaccord
- ◯ D'accord
- ◯ Tout à fait d'accord

16. Si j'ignore quelqu'un qui agit de manière suspecte sur mon lieu de travail, rien de mal ne peut arriver *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Ni d'accord ni en désaccord
- ◯ D'accord
- ◯ Tout à fait d'accord

17. Je sauvegarde régulièrement tous les fichiers et les données (sur le serveur, sur l'ordinateur, dans le drive etc.) *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Ni d'accord ni en désaccord
- ◯ D'accord
- ◯ Tout à fait d'accord

18. Accepter que certaines contraintes (par exemple, changer mon mot de passe régulièrement, faire des sauvegardes) sont nécessaires pour sécuriser des informations importantes. *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Ni d'accord ni en désaccord
- ◯ D'accord
- ◯ Tout à fait d'accord

19. Je sais qu'elles sont mes responsabilités en matière de sécurité de l'information *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Ni d'accord ni en désaccord
- ◯ D'accord
- ◯ Tout à fait d'accord

20. Je crois avoir une responsabilité concernant la protection du système d'information de l'entreprise *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Ni d'accord ni en désaccord
- ◯ D'accord
- ◯ Tout à fait d'accord

21. La sécurité des systèmes d'information est avant tout une question technique (elle concerne principalement la division informatique) *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Ni d'accord ni en désaccord
- ◯ D'accord
- ◯ Tout à fait d'accord

22. Je connais les aspects de sécurité des informations liés à ma fonction professionnelle (par exemple, comment choisir un mot de passe ou gérer des informations confidentielles) *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Ni d'accord ni en désaccord
- ◯ D'accord
- ◯ Tout à fait d'accord

23. Je crois que les exigences de sécurité des systèmes d'information devraient être intégrées à mes tâches quotidiennes (La manière dont je gère les informations quotidiennement) *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Ni d'accord ni en désaccord
- ◯ D'accord
- ◯ Tout à fait d'accord

24. Je pense qu'il est nécessaire d'engager les gens dans la sécurité des systèmes d'information *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Ni d'accord ni en désaccord
- ◯ D'accord
- ◯ Tout à fait d'accord

25. Mes collègues font preuve d'engagement envers la sécurité des systèmes d'information *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Ni d'accord ni en désaccord
- ◯ D'accord
- ◯ Tout à fait d'accord

26. Je sais qu'est ce que l'RGPD *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Ni d'accord ni en désaccord
- ◯ D'accord
- ◯ Tout à fait d'accord

27. Je sais qu'est ce que l'hameçonnage ou le phishing *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Ni d'accord ni en désaccord
- ◯ D'accord
- ◯ Tout à fait d'accord

28. Je sais comment éviter l'hameçonnage ou le phishing (les bases/des bonnes pratiques) *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Ni d'accord ni en désaccord
- ◯ D'accord
- ◯ Tout à fait d'accord

29. Je sais qu'est ce qu'un rançongiciel *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Ni d'accord ni en désaccord
- ◯ D'accord
- ◯ Tout à fait d'accord

30. Je sais comment éviter un rançongiciel (les bases/des bonnes pratiques) *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Ni d'accord ni en désaccord
- ◯ D'accord
- ◯ Tout à fait d'accord

31. J'ai lu la charte de sécurité des systèmes d'information *

Une seule réponse possible.

- ◯ D'accord
- ◯ Pas d'accord

32. Je pense que la charte de sécurité des systèmes d'informations est pratique et m'aide à protéger les informations *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Ni d'accord ni en désaccord
- ◯ D'accord
- ◯ Tout à fait d'accord

33. J'ai participé à une formation et/ou j'ai eu des cours (en ligne par exemple) lié à la sécurité des systèmes d'information *

Une seule réponse possible.

- ◯ Pas d'accord
- ◯ D'accord

34. Je pense que la formation que j'ai reçu est intéressante *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Ni d'accord ni en désaccord
- ◯ D'accord
- ◯ Tout à fait d'accord

35. J'ai apprécié(e) le quiz réalisé pendant la formation *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Ni d'accord ni en désaccord
- ◯ D'accord
- ◯ Tout à fait d'accord

36. Je préfère une formation ludique (Jeux, échanges) sur la sécurité qu'une formation classique (formats traditionnels) *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Ni d'accord ni en désaccord
- ◯ D'accord
- ◯ Tout à fait d'accord

37. Je pense qu'après la formation, j'ai amélioré mes comportements de sécurité *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Ni d'accord ni en désaccord
- ◯ D'accord
- ◯ Tout à fait d'accord

38. Je pense qu'après la formation, j'ai remarqué une amélioration des comportements de mes collègues (confidentialité des données et des mots de passe, plus de vigilance) *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Ni d'accord ni en désaccord
- ◯ D'accord
- ◯ Tout à fait d'accord

39. J'ai lu l'affiche exposée dans l'entreprise sur la sauvegarde des données *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Ni d'accord ni en désaccord
- ◯ D'accord
- ◯ Tout à fait d'accord

40. Je fais plus attention à la sauvegarde de mes données après la lecture de l'affiche sur les sauvegardes *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Ni d'accord ni en désaccord
- ◯ D'accord
- ◯ Tout à fait d'accord

41. J'ai lu la brochure de sensibilisation à la sécurité distribuée à la fin de la formation *

Une seule réponse possible.

- ◯ Pas d'accord
- ◯ D'accord

42. Je pense que cette brochure n'est pas intéressante *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Ni d'accord ni en désaccord
- ◯ D'accord
- ◯ Tout à fait d'accord

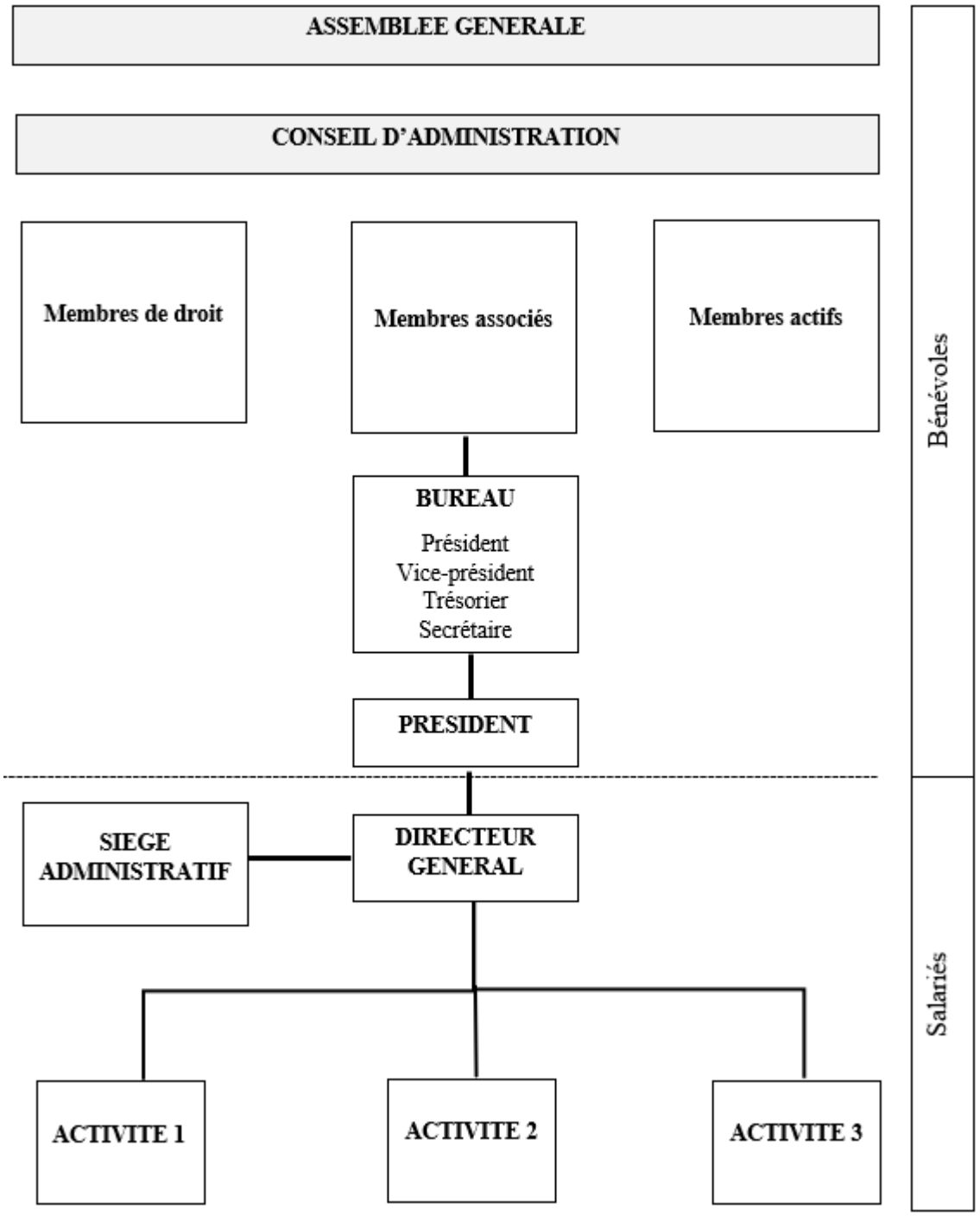
43. Après la lecture de cette brochure j'ai senti plus responsable à la sécurité des données *

Une seule réponse possible.

- ◯ Pas du tout d'accord
- ◯ Pas d'accord
- ◯ Ni d'accord ni en désaccord
- ◯ D'accord
- ◯ Tout à fait d'accord

44. Merci d'exprimer votre opinion, vos expériences, vos propositions etc. à propos la sécurité des informations. *

Annexe 6 : Organigramme de l'entreprise G (Association)



Annexe 7 : Guide d'entretien direction

Guide d'entretien (Responsables)

Point de départ de l'entretien :

1) Pouvez-vous vous présenter s'il vous plaît ?
2) Depuis quand êtes-vous dans l'entreprise ? Votre âge ?
3) Quel est votre poste ou votre fonction au sein de l'entreprise ?

Thèmes à évoquer au cours de l'entretien

○ Thème 1 : Facteurs exogènes

- **Contexte règlementaire**

1) Appliquez-vous les normes ISO relatives au Management de la sécurité des SI (Comme ISO 27001) ?

(Si oui) : Quel est votre objectif de l'utilisation de cette norme ? Avez-vous obtenus la certification ?

2) Avez-vous signés des chartes, (comme la charte d'utilisation des moyens informatiques) ? Que pensez-vous de leur utilité ?

3) Avez-vous déjà entendu parler du règlement général sur la protection des données (RGPD) ?
Est-ce que vous avez lancé des actions de conformité ?
-Est-ce que vous avez mis en place registre de traitements des données personnelles ?

- **Prestataires des services informatiques**

1) Que pensez-vous du rôle de votre prestataire informatique ?

2) Est-ce que vous avez signé une charte cybersécurité avec lui ? Et en quoi cette charte consiste ?

○ Thème 2 : Facteurs endogènes

- **Analyse des risques (Audit par Cobit)**

1) Appliquez-vous un référentiel ou une méthode d'analyse des risques informatiques ?

2) La gestion des risques informatique est-elle pleinement intégrée aux processus de management, en interne et en externe ? (Avec quelle fréquence ? périodes/an ?)

3) Procédez-vous à l'évaluation des risques (Probabilité, niveau de risque : très faible, faible, moyen, fort, très fort) ?

4) Pour les risques informatiques critiques développer vous des plans d'actions ? Et est-ce que ces plans d'actions ont été mis en œuvre ? (PRA, PCA)

5) Surveiller vous l'exécution des plans et est-ce que vous rapportez tout écart au management ?

6) Est-ce qu'il y'a un responsable de la gestion des risques informatiques ?

- **Formation et sensibilisation**

1) -Est-ce que vous avez mis en place une formation à la sécurité informatique ?
Si oui,
-Depuis quand ? La fréquence de cette formation ? Budget engagé ? Public cible ? (Cadre, salariés, toutes les équipes…) Contenu de la formation ? (Consultation des supports si possible) Efficacité de cette mesure ? (sur les résultats, sur le public cible, amélioration ?)

2) Est-ce que l'inscription à cette formation est volontaire ou imposée ?
Dans le cas d'une inscription volontaire à votre avis quelles sont les motivations des bénéficiaires de la formation ?

3) -Est-ce que vous sensibiliser vos salariés et vos collaborateurs à la sécurité ? (Exp : affiches,
Tapis de souris, stylos avec slogans de sécurité)
Si, oui :
-De quelle manière ? Budget engagé ? Public cible ? Efficacité de cette mesure ?

○ Thème 3 : Support de la direction :

1) Qui est/sont les responsable (s) des mesures sécuritaires ? (en terme de décision)

2) Quel budget approximatif avez-vous engagé afin de mettre en place ces mesures ? Pensez-vous que la direction prête à augmenter ce budget en cas de besoin ?

-Que pensez-vous du rôle qu'exerce la direction pour impliquer vos employés et vos collaborateurs dans le respect de ces mesures ?

o Thème 4 : Niveau de la SSI

1) Comment gérer vous les identités et les autorisations des utilisateurs des SI ? (façon standardisée, badge, codes d'accès…).

2) Est-ce que vous testez régulièrement la sécurité de vos SI ? (Tests d'intrusion, détection des activités inhabituelles/anormales…) Si, oui : (Avec quelle fréquence ? périodes/an ?)

3) Gérez-vous les clefs de chiffrement afin de garantir leur protection contre toute modification ou divulgation non autorisée ?

4) Mettez-vous en place des mesures de prévention, détection et neutralisation dans l'ensemble de l'entreprise pour protéger les SI et la technologie contre les logiciels malveillants ?

(Correctifs de sécurité et des anti-virus à jour)

5) Mettez-vous en œuvre des techniques de sécurité et des procédures de gestion associées pour autoriser et contrôler les flux d'informations entre réseaux ?

(Ex. pare-feu, dispositifs de sécurité, compartimentage réseau, détection d'intrusion)

6) Comment faites-vous circuler les échanges de données sensibles ?

7) Pensez-vous que les utilisateurs (Salariés, collaborateurs) du SI respectent les mesures de sécurités mises en places ?

Si oui, selon vous quel est le facteur ou les facteurs qui influencent leurs comportements ?

Si non, selon vous qu'elle est la cause de la non implication des utilisateurs ?

Conclusion de l'entretien :

Je vous remercie pour ces éléments de réponses.

-Connaissez-vous d'autres PME qui peuvent être sensibles à la SSI ?

- Est-il possible que je fasse des entretiens avec quelques salariés de votre entreprise ?

Guide d'entretien (Dirigeant)

Point de départ de l'entretien :

1) Pouvez-vous se présenter s'il vous plaît ? Votre âge ?
2) Quel est le nombre de vos collaborateurs dans l'entreprise ?

Thème 1 : Support de la direction pour la SSI

1) Quand vous entendez « sécurité des SI» qu'est-ce que cela vous évoque ?
2) Est-ce que ça vous intéresse comme sujet ?
3) Est-ce que vous avez engagés des mesures sui concernent la sécurité des SI dans votre entreprise ?
4) Quel est le responsable des mesures sécuritaires mise ou à mettre en place ? (En termes de décision)
5) Quel budget approximatif avez-vous engagé afin de mettre en place des mesures sécuritaires ?
6) Est-ce que vous êtes prêts à augmenter ce budget dans le futur ou en cas de besoin ?
7) Que pensez-vous du rôle que vous exercez pour impliquer vos collaborateurs dans le respect des mesures sécuritaires ?

o Thème 2 : Facteurs exogènes

- **Contexte règlementaire**

1) Appliquez-vous les normes ISO relatives au Management de la sécurité des SI (Comme ISO 27001) ?

(Si oui) : Quel est votre objectif de l'utilisation de cette norme ? Avez-vous obtenus la certification ?

2) Avez-vous déjà entendu parler du règlement général sur la protection des données (RGPD) ?

Est-ce que vous avez lancé des actions de conformité ?

- **Prestataires des services informatiques**

1) Est-ce que le service informatique est géré au sein de votre entreprise ou il est externalisé ?

2) Que pensez-vous du rôle de votre prestataire informatique ? (En termes de service et niveau de sécurité informatique)

3) Est-ce que vous avez signé une charte qui concerne la sécurité informatique avec lui ? Et en quoi cette charte consiste ?

○ Thème 3 : Facteurs endogènes

- **Analyse des risques (Audit par Cobit)**

1) Appliquez-vous un référentiel ou une méthode d'analyse des risques informatiques ?

2) La gestion des risques informatique est-elle pleinement intégrée aux processus de management ?

3) Procédez-vous à l'évaluation des risques informatiques (Probabilité, niveau de risque : très faible, faible, moyen, fort, très fort) ?

4) Pour les risques informatiques critiques développer vous des plans d'actions* ? Et est-ce que ces plans d'actions ont été mis en œuvre ?

*(PRA : Un plan de reprise d'activité, PCA : Plan de continuité d'activité)

- **Formation et sensibilisation**

1) -Est-ce que vous avez mis en place une formation à la sécurité informatique pour vos collaborateurs ?
-Depuis quand ? -Budget engagé -Public cible ? (Cadre, salariés, etc.)

2) Est-ce que vous sensibiliser vos salariés et vos collaborateurs à la sécurité ? (Exp : affiches)
Si, oui : -De quelle manière ?

- **Thème 4 : Niveau de la SSI**

1) Comment gérer vous les identités et les autorisations des utilisateurs des SI ? (façon standardisée, badge, codes d'accès…).

2) Est-ce que vous testez régulièrement la sécurité de vos SI ? (Tests d'intrusion, détection des activités inhabituelles/anormales…)

4) Mettez-vous en place des mesures de prévention, détection et neutralisation dans l'ensemble de l'entreprise pour protéger les SI ?

(Correctifs de sécurité et des anti-virus à jour)

5) Mettez-vous en œuvre des techniques de sécurité et des procédures de gestion associées pour autoriser et contrôler les flux d'informations entre réseaux ?

(Ex. pare-feu, dispositifs de sécurité, compartimentage réseau, détection d'intrusion)

6) Pensez-vous que les utilisateurs du SI au sein de votre entreprise respectent les mesures de sécurités mise en place ?

7) Si oui, selon vous quel est le facteur ou les facteurs qui influencent leurs comportements ?

Conclusion de l'entretien :

Je vous remercie pour ces éléments de réponses.

- Est-il possible que je fasse des entretiens avec quelques salariés de votre entreprise ? (15 min/salarié) pour mesurer leur culture sécuritaire.

-Connaissez-vous d'autres PME qui peuvent être sensibles à la SSI ?

Annexe 8 : Guide d'entretien utilisateurs du SI

Point de départ de l'entretien :

1) Pouvez-vous se présenter s'il vous plaît
2) Vous êtes dans l'entreprise depuis quand ?
3) Quel est votre poste ou votre fonction au sein de l'entreprise ?

o Thème 1 : La culture sécurité

• Propriété de sécurité (Basic assumptions and beliefs)

1) -Quand vous entendez « sécurité des SI » qu'est-ce que cela vous évoque ?

2) Est-ce que ça vous intéresse comme sujet ?

3) -Selon vous, qui doit être responsable d'assurer la sécurité des SI et la confidentialité des données au sein de votre entreprise ?

*Si la personne mentionne sa responsabilité :

4) -Dans quelle mesure, sentez-vous responsable de la sécurité des SI de votre entreprise ?

5) -Quel est votre rôle en matière de sécurité ? Et qu'est-ce qui vous motive à assurer ce rôle ?

Relance : ***En fonction des mots employés par le/la répondant(e) demander des précisions pour mieux cerner les motivations*** : Vous avez parlé de […], qu'entendez-vous par là ?, pouvez-vous préciser s'il vous plaît ?

*Si la personne ne mentionne pas sa responsabilité :

6) -Sentez-vous obligé à respecter les mesures sécuritaires mises en place au sein de votre entreprise ?

Pour qu'elle raison ?

8) - Pensez-vous que vous contribuez positivement à la Sécurité des SI de votre entreprise ?

• Conscience (Collective value, norms and knowledge)

1) -Qu'est-ce que le piratage informatique pour vous ?

2) -Connaissez-vous d'autres types de risques et de menaces qui peuvent influencer votre poste de travail ou les systèmes de votre entreprise ? (hameçonnage, ingénierie sociale, spam, virus…)

3)-Avez-vous une idée comment se protéger contre ses risques et ses menaces ?

4)-Est-ce que vous avez déjà rencontré un problème de sécurité ?

Si oui, pouvez-vous nous raconter ce qui est arrivé et comment avez-vous réagi ?

5)-A votre avis êtes-vous capable de faire face à d'autres problèmes de sécurité ?

6)-A qui s'adresser vous en cas de problème non résolu par vous-même ? (Collègues, responsables…)

7)-Est-ce que votre entreprise met en place des mesures sécuritaires pour protéger les systèmes ? Pouvez-vous citez ses mesures ?

Que pensez-vous de ses mesures ? (utiles/inutiles, suffisantes/insuffisantes, faciles/difficiles à appliquer…)

- **Conformité (Artefacts and creations)**

1)-Participez-vous à des formations liés à la sécurité des SI ?

Si oui, comment évaluer vous cette formation ? Qu'est-ce qu'elle vous a apporté de plus que ce soit dans votre travail ou votre vie quotidienne ?

2)-S'il y'a des chartes de sécurité ou des clauses contractuelles :Avez-vous déjà signé la charte… ou avez-vous déjà lu la politique de sécurité… ? Quelles idées avez-vous pu en retenir ?

- **Thème 2 : Comportement sécuritaire**

1) -Combien de fois changer vous vos mots de passe, (fréquence) ? (poste de travail, code bancaire, portable, mails, réseaux sociaux…)

2)-Vos mots de passes réfèrent ils à des éléments personnels (Date ou lieu de naissance, date mariage…) ?

3)-Faites-vous des mises à jour régulières (Logiciels, applications, poste de travail…) ? (fréquence)

4)-Sauvegarder vous les données régulièrement ? (fréquence)

5)-Avez-vous divulgué vos mots de passe ou des informations confidentiels à des tiers non concernés ? Pour quelle raison ?

6) -Est-ce que vous pensez que vous avez une culture en sécurité informatique ?

7) Selon vous, qu'est ce qui pourrait être mis en place par votre entreprise pour renforcer la culture sécurité informatique des collaborateurs ?

Conclusion de l'entretien : Je vous remercie pour ces éléments de réponse.

Annexe 9 : Gestion des CLES (site) Entreprise G

Le trousseau de clés comprend X clés : Porte A, Porte B,…

	Clés remises				Clés rendues			
N° Clé	**Date**	**Nom**	**Prénom**	**Signature**	**Date**	**Nom**	**Prénom**	**Signature**
1								
2								
5								
X								

DOCTORAT BRETAGNE LOIRE ECONOMIE ET GESTION

UBO Université de Bretagne Occidentale

Titre : Conception et mise en œuvre d'une culture sécurité des systèmes d'information : Le cas des PME

Mots clés : Culture sécurité, sécurité des systèmes d'information (SSI), comportements de sécurité, PME.

Résumé : Cette recherche vise à comprendre, conceptualiser et insuffler la culture sécurité des utilisateurs des systèmes d'information (SI) dans les PME, puisque la revue de littérature dans ce domaine a mis en évidence que les employés représentent le « maillon faible » de la sécurité des systèmes d'information (SSI). Dans un premier temps, nous avons réaliser une intervention au sein d'une PME, cette intervention consiste à sensibiliser et former un groupe d'utilisateurs sur la sécurité des SI ensuite évaluer l'effet de cette intervention sur la culture et les comportements de ces utilisateurs. Cette évaluation a montré une amélioration au niveau de la culture et des comportements des utilisateurs. Néanmoins, après des allers retours entre théorique et pratique, il s'avère que l'amélioration de la culture sécurité ne se limite pas uniquement à une sensibilisation et/ou une formation mais dépend aussi d'autres facteurs, d'où la nécessité de la prise en compte de la culture sécurité dans sa globalité et d'analyser cette culture dans une logique plus systémique. A cet effet, nous avons dans un deuxième temps élaborer notre modèle conceptuel de la culture sécurité à partir de la revue de littérature et de nos premiers résultats du terrain. Ensuite, pour confronter notre modèle conceptuel au terrain, nous avons réaliser une étude qualitative à travers l'étude de cas de huit PME en réalisant 32 entretiens semi directifs avec la direction et les utilisateurs SI de chaque PME étudiée. Les résultats de cette étude ont confirmé que des facteurs exogènes (Contexte légal, le secteur d'activité, etc.), des facteurs endogènes (gestion des risques, formation et sensibilisation) et le dirigeant de la PME influencent positivement la culture sécurité des utilisateurs du SI et en conséquence, une culture de sécurité positive est favorable à créer un comportement lié à la sécurité. D'autres facteurs tels que l'âge de l'utilisateur et son poste ont émergé de cette étude comme facteurs modérateurs dans la relation entre la culture sécurité de l'utilisateur et son comportement effectif.

Title : Design and implementation of an information systems security culture : the case of SMEs

Keywords : security culture, information systems security (ISS), security-related behaviour, SMEs.

Abstract : This research seeks to understand, conceptualise and instil the security culture of information systems (IS) users in SMEs, as the literature review in this field has highlighted the fact that employees represent the "weak link" in information systems security (ISS). First, we conducted an intervention within an SME; this intervention consists in raising awareness and training a group of users on IS security and then, in evaluating the effect of this intervention on the culture and behaviours of these users. This assessment showed an improvement in the culture and behaviour of the users. Nevertheless, after going back and forth between theory and practice, it turns out that the improvement of the security culture is not limited to awareness-raising and/or training alone, but also depends on other factors, hence the need to take into account the security culture in its entirety and to analyse this culture in a more systemic perspective. For this purpose, in a second stage, we developed our conceptual model of safety culture based on the literature review and our first field results. Then, in order to confront our conceptual model with reality, we carried out a qualitative study through the case study of eight SMEs, by conducting 32 semi-directive interviews with the leadership and the IS users of each SME studied. The results of this study confirmed that exogenous factors (legal context, sector of activity, etc.), endogenous factors (risk management, training and awareness) and the SME leader positively influence the security culture of IS users and, as a result, that a positive security culture is beneficial in creating security-related behaviour. Other factors, such as the user's age and position, emerged from this study as moderating factors in the relationship between the user's security culture and actual behaviour.