La mise en œuvre d'une culture sécurité des systèmes d'information au sein des PME : à la recherche de la performance

Olfa Ismail
Université de Nantes, laboratoire d'économie et de management de Nantes-Atlantique,
Chemin de la Censive du Tertre, 44322 NANTES Cedex 3, France
Olfa.Ismail@univ-nantes.fr

Mots-clés : Culture, comportements, sécurité des systèmes d'information (SSI), intervention, étude de cas.

Résumé : Cette recherche vise à comprendre et conceptualiser 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. 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 tels que le contexte légal, la gestion des risques 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 ont émergé de cette étude comme facteurs modérateurs dans la relation entre la culture sécurité de l'utilisateur et son comportement effectif.

1. Introduction

Selon une étude faite par Clusif (2022) toutes les entreprises interrogées tous secteurs confondus et quelle que soit leur taille confirment, que le système d'information (SI) 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 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.

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). 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. 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. Dans l'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 (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. De plus, la culture sécurité a de sérieux problèmes concernant sa mise en œuvre dans les PME (Hutchinson et al, 2014) 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). Les PME présentent donc de nombreux intérêts théoriques et pratiques. Pour ces raisons, nous posons la question suivante : comment peut-on diffuser et renforcer une culture sécurité des systèmes d'information en PME afin de garantir sa pérennité ?

2. Revue de littérature

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 ». (Auteur).
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. 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.

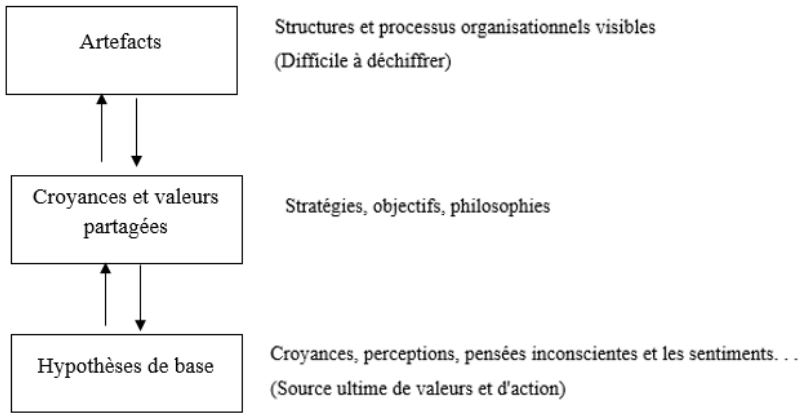

Figure 1 : Niveaux de culture (Schein, 1985)

-**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.

A travers la littérature, il existe trois facteurs qui constituent une culture sécurité des SI (Alnatheer et al 2012, et Tolah et al, 2017) à savoir :

-**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.
-**Conscience de sécurité** : 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.
-**Conformité à la sécurité** : 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.

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 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 suivante :

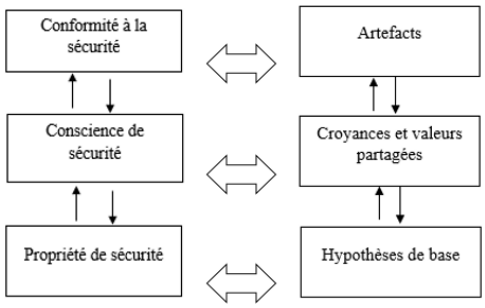

Figure 2 : Positionnement des facteurs qui constituent la culture sécurité des SI sur les trois niveaux de culture

3. Méthodes de recherche et résultats R3.10 R1.08

Après une première revue de littérature, nous avons réaliser une intervention au sein d'une PME (2017-2018) . Nous avons proposé au dirigeant de cette PME, 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, 1979 ; Moisdon, 2010 ; Savall et Zardet, 1996, 2004 ; David, 2000), surtout que nous avons été en phase d'exploration 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 (3.1) nous allons développer les étapes et les résultats de cette intervention réalisée. A travers cette intervention, 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, dans cette optique nous avons passer à une deuxième revue de littérature plus profonde pour proposer un modèle conceptuel de la culture sécurité en PME (Titre 3.2), 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 détails de cette étude qualitative seront présentés dans le titre (3.3).

3.1. Etude 1 : Intervention au sein d'une PME

Nous nous sommes inspirés de la démarche d'une recherche intervention, 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 […]* ». La figure 2 présente les quatre étapes de notre intervention qui seront détaillés ci-dessous :

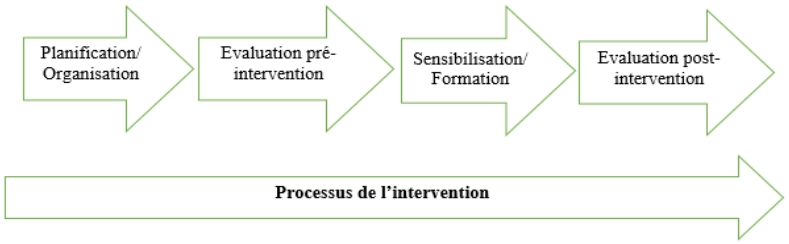

Figure 3 : Les étapes du déroulement de l'intervention

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 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 questionnaire « Avant intervention » a été transmis vers mi-octobre 2017 aux participants, qui représentent les utilisateurs des SI de l'entreprise. Et en quelques jours, nous avons reçu les réponses des 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 2 : Le déroulement de la formation à la sécurité des SI

Le deuxième volet de cette intervention, c'est la sensibilisation à la sécurité des SI à travers une brochure (Annexe1) 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 2) 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

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. 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 ci-après, 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.

Résultats de l'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. A titre d'exemple le tableau suivant représente la comparaison de quelques items du questionnaire entre l'avant et l'après :

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
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

Tableau 3 : Comparaison entre réponses avant et après intervention

En plus, la personne responsable des sauvegardes de données au sein de la PME 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.

Discussion des résultats de l'intervention

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.).

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. 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.

3.2. Approfondissement de la littérature et proposition d'un modèle conceptuel de la culture sécurité en PME

Suite à nos résultats issus de l'intervention, nous sommes passé à une revue de littérature plus approfondie sur la culture et les comportements de sécurité et plus particulièrement dans le contexte des PME. Cette revue nous a permis d'identifier les facteurs qui peuvent influencer la culture sécurité et par la suite les comportements à savoir :

-**Le contexte réglementaire et légal** : qui 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).
-**Rôle des prestataires informatiques** : 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. Dojkovski (2007) ; Barlette (2005).
-**Appartenance à un Secteur d'activité** : 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).
-**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, Tolah et al (2017).
-**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, Alnatheer et al (2012) ; Tolah et al (2017).
En plus de ces facteurs, nous avons déjà identifié précédemment l'influence de la formation et la sensibilisation (facteurs qui influencent la culture et les comportements) et les facteurs qui composent la culture sécurité à savoir la propriété la conscience et la conformation ce qui nous mène à proposer le modèle conceptuel suivant :

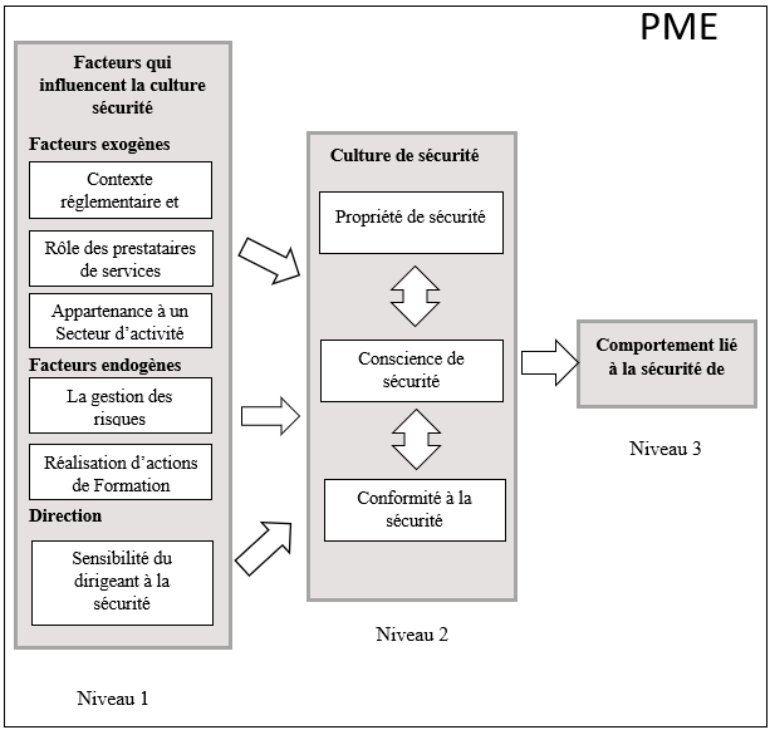

Figure 4 : le modèle conceptuel de la recherche

Afin de confronter notre modèle à la réalité du terrain nous allons passer à notre deuxième étude qualitative les études de cas.

3.3. Etude 2 : Des études de cas

Selon Kotulic et Clark (2004), une méthode privilégiant des entretiens en face à face doit être adoptée dans un domaine aussi sensible que la sécurité. Nous avons réalisé des études de cas

au sein de huit PME françaises, à travers 32 entretiens semi-directifs avec les dirigeants et responsables de PME (Guide d'entretien spécifique dirigeants et responsables) et avec les utilisateurs des systèmes d'informations (Guide d'entretien spécifique utilisateurs). Le Tableau 4 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 4 : Caractéristiques des PME étudiées

Nous avons utilisé le logiciel Nvivo afin de coder nos données, d'avoir ensuite une analyse plus cohérente et d'aller plus loin dans la recherche de relations entre concepts. Les résultats obtenus suite à cette analyse de données seront exposés ci-après.

Résultats des études de cas

Typologie des cas étudiés : Nous avons fixé 3 niveaux de sécurité à partir des mesures réglementaires et légales (normes ISO, RGPD, chartes et clauses), des mesures organisationnelles (gestion des risques, formation et sensibilisation), et 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 sur 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).
-**Niveau 3** : Entreprises A et G avec des mesures de sécurité en place et une forte sensibilité de la direction à la sécurité.

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.

Typologie des utilisateurs : Dans cet élément, nous allons estimer en premier lieu, 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 (Intérêt pour la sécurité, responsabilité de sécurité), conscience (Connaissance des mesures de sécurité prises, Autres types de menaces, comment se protéger) et conformité (participation à une formation, programme de sensibilisation). Et en deuxième lieu, le niveau de comportements lié à la sécurité (Changement de mot de passe, référence à des éléments personnels, sauvegarde des données).

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)

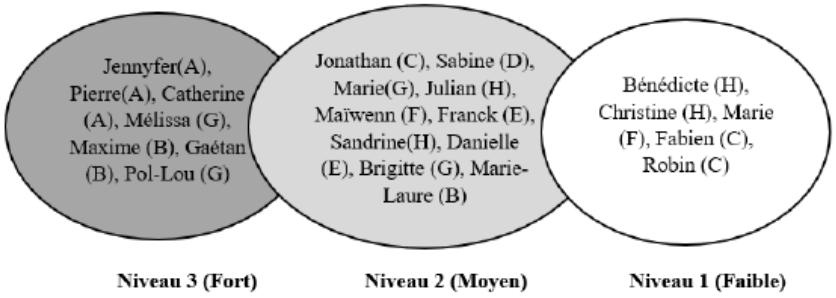

Figure 5 : Classification des utilisateurs selon leurs niveaux de CSSI

Après l'évaluation des comportements liés à la 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)

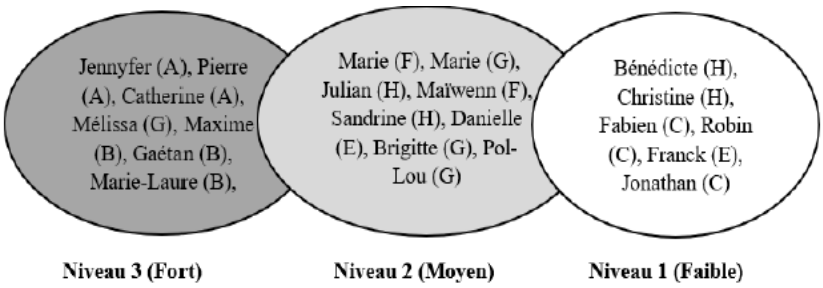

Figure 6 : Classification des utilisateurs selon leurs niveaux de comportements relatifs à la SSI

Parmi les freins aux comportements liés à la sécurité exprimés par les utilisateurs, nous citons :

-Changement des mots de passe : par peur d'oublier le mot de passe, exemple de verbatim : *'' 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)
-Mots de passe qui réfèrent à des éléments personnels : facile à retenir, exemple de verbatim :
''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)

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 d'en tirer des conclusions.

4. Discussion des résultats

4.1 Le contexte règlementaire et légal

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). 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).

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.

4.2 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 (entreprises D et G), Une confiance limitée ou une insatisfaction (entreprise B), Un rôle de conseil et de support technique, (entreprises C, D, G, E et F), Rôle d'RSSI et DPO (entreprise A), et une relation non stable avec le prestataire (entreprise H). 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 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 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.

4.3 Le secteur d'activité

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. 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).

4.4 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. 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.

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.

4.5 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, et c'est l'entreprise qui a le niveau de sécurité le plus élevé. 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).

4.6 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. 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).

4.7 Relation culture-comportement

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. 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.

4.8 Émergence d'autres facteurs

-Différence entre générations (âge de l'utilisateur) : Lors des interviews, nous constatons que cinq salariés évoquent la différence entre les générations par exemple « *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).

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.

Selon une recherche réalisée par Miltgen et 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.

- Le poste occupé par l'utilisateur

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. 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.

5. Conclusion

A travers cette recherche nous avons mobiliser en premier lieu une recherche intervention au sein d'une PME afin vérifier l'impact d'une sensibilisation et une formation à la sécurité des SI sur la culture et les comportements des utilisateurs. 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. Donc nous avons approfondi notre revue de littérature pour déterminer les facteurs qui peuvent influencer cette culture de sécurité, en proposant un modèle conceptuel de la culture sécurité qui représentent les facteurs qui influencent et les facteurs qui composent cette culture et ensuite l'effet sur les comportements. Pour confronter notre modèle au terrain, nous avons réalisé des études de cas dans huit PME françaises à travers des entretiens avec les directions, les responsables et les salariés. Cette deuxième étude a montré que des facteurs comme l'engagement de la direction, la gestion des risques etc. ont une influence notable sur la culture de l'utilisateur du SI et que plus la culture est élevée plus ont a tendances à identifier des comportements de sécurité élevés et inversement. De plus, d'autres facteurs ont émergés de cette étude à savoir le poste et l'âge de l'utilisateur qui peuvent jouer un rôle modérateur entre la culture et le comportement. A notre connaissance, il n'a pas d'autres études qui ont testé ces facteurs dans le cadre des PME. Néanmoins, 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.

6. Bibliographie

Alnatheer, M., Chan, T., Nelson, K. (2012). Understanding And Measuring Information Security Culture. *Pacific Asia Conference on Information Systems*, pp144.

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. (2014). A Conceptual Model to Understand Information Security Culture. *International Journal of Social Science and Humanity*, Vol. 4, No. 2, March 2014.

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., Jaouan, A., (2019). Information security in SMEs: determinants of CEOs' protective and supportive behaviors. *Système d'information et Management*, N° 3 – VOL. 24, 2019.

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.

Cappelletti, L. (2010). La recherche-intervention: quels usages en contrôle de gestion? », *Crises et nouvelles problématiques de la Valeur*, May 2010, Nice, France.

Clusif. (2020). Menaces informatiques et pratiques de sécurité en France, *Club de la sécurité informatique Français*, édition Juin 2020.

CPME (2019), *La cybersécurité des entreprises (-50 salariés) : Enquête*, Janvier 2019.

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.

Connolly L Y., Lang M ., Gathegi J., Tygar D J. (2017), Organizational Culture, Procedural Countermeasures and Employee Security Behaviour: A Qualitative Study, *Information and Computer Security*, Vol. 25 Issue: 2.

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, Eloff (2010). A framework and assessment instrument for information security culture, *computers & security* 29 (2010) 196-207.

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.

David, A. (2000), *La recherche intervention, un cadre général pour les sciences de gestion ?*, *IXème Conférence de l'AIMS*, Montpellier, 24-26 mai.

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.

Flores W R., Ekstedt M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness, Computers and Security, 2016, 59:26-44.

Guo, K. H., Yuan, Y. (2012). The effects of multilevel sanctions on information security violations : A mediating model. *Information & Management*, Volume 49, Issue 6, October 2012, Pages 320-326.

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.

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.

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.

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.

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.

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.

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.*

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*, Pages 103-125.

Schein EH (1985), *Organizational culture and leadership*, San Francisco, Jossey-Bass, Publishers, 1985, 358 pages.

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.

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. (1979), *Reconstruire l'entreprise*, Dunod.

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.

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.

Srinivas J., Kumar Das A., Kumar N. (2018), Government regulations in cyber security: Framework, standards and recommendations, Future Generation Computer Systems, Vol. 92, March 2019, p.178-188.

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.

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.* Volume: 9 issue: 2, page(s): 117-129.

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.

7. Annexes

Annexe 1 : brochure de sensibilisation à la sécurité des SI

Annexe 2 : Affiche de sensibilisation aux sauvegardes de données