Construction d'un modèle théorique pour l'évaluation de la culture sécurité des systèmes d'information en PME

Olfa Ismail, André Mourrain, Christian Cadiou

Construction d'un modèle théorique pour l'évaluation de la culture sécurité des systèmes d'information en PME

Olfa Ismail*

André Mourrain**

Christian Cadiou****

IAE de Bretagne Occidentale, Université de Brest, France Laboratoire LEGO

*olfa.ismail@etudiant.univ-brest.fr /** andre.mourrain@univ-brest.fr / ***Christian.Cadiou@univ-brest.fr

Résumé :

En 2019 selon une enquête du CPME[1] 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. En ayant une culture sécurité des systèmes d'information (CSSI) efficace où les employés protègent les actifs informationnels, les petites et moyennes entreprises (PME) pourraient améliorer la sécurité de leurs systèmes d'information (Dojkovski et Al 2007). Cependant, les recherches antérieures ont largement ignoré le développement d'une telle culture pour les PME. L'objectif de cette recherche est de répondre à la question : « Comment évaluer la maturité de la culture sécurité des SI dans les PME ». Cette communication propose un modèle théorique qui doit permettre d'évaluer la maturité de la culture SSI d'une PME. Ce modèle est construit en se basant sur la théorie des trois niveaux de la culture sécurité de Schlienger et Teufel (2003) adapté de Schein (1985). Dans cette communication nous présentons également notre méthode de recherche et les cas prévus. Par la suite ce modèle fera l'objet d'une validation par des études de cas.

Mots clés :

Culture sécurité, PME, sécurité des SI, comportement sécuritaire, maturité de la culture.

[1] CPME : Confédération des Petites et Moyennes Entreprises.

1. Introduction :

Bien que les entreprises investissent de plus en plus dans la sécurité de leurs infrastructures informatiques, et que des protections se mettent en place les intrusions et les incidents se multiplient. Notamment une étude Clusif (2018)[2], montre que les incidents les plus fréquemment signalés ont eu pour cause des vulnérabilités de l'intérieur de l'entreprise.

Cette étude constate des problèmes de comportement humain, avec un manque de compréhension des menaces et des risques sous-jacents. D'autres études et recherches montrent qu'une grande part des pertes provoquées par un sinistre informatique a pour origine les propres collaborateurs de l'entreprise (Deloitte 2018[3], Wang et al, 2015). Ceux-ci 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 attention particulière à la 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 de l'information doit être considérée dans le cadre d'un programme de sécurité de l'information permettant notamment d'orienter le comportement des employés. L'instauration d'une telle culture peut contribuer à la protection de l'information et minimiser le risque que pose ce comportement. (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. Par conséquent, la création d'une culture de la sécurité de l'information est nécessaire pour une gestion efficace de la sécurité de l'information.

La question de la culture sécurité des SI, révèle plusieurs intérêts, premièrement sur le plan managérial, il devient très intéressant de comprendre quels sont les composants de la culture sécurité, existe-t-elle réellement au sein des entreprises ? Dans le cas d'une réponse positive de chercher les moyens d'améliorer cette culture et dans le cas inverse de chercher les moyens qui favorisent la naissance et la formation d'une culture sécurité.

Existe-t-il des modèles ou des théories concernant cette culture sécurité ? Quels sont les moyens de l'évaluer pour pouvoir l'améliorer ? Et quels en sont les déterminants ?

Galletta et Polak (2003) ont souligné la valeur potentielle de l'adoption d'une approche socioculturelle de la gestion de la sécurité de l'information. Leur étude a révélé que la culture des superviseurs peut être très influente dans la gestion des abus internes liés à l'internet. Cependant, même si des progrès ont été réalisés à l'échelle mondiale dans le domaine de l'enculturation de la sécurité de l'information, il faut en faire plus (Ernst et Young, 2006).

---

[2] CLUSIF (2018), Menaces informatiques et pratiques de sécurité en France, Edition 2018, 104p.
[3] Deloitte, (2018) : « Enjeux cyber 2018 : L'évolution de la menace cyber ».
file:///C:/Users/ASUS/Downloads/deloitte_enjeux-cyber-2018_janv-2018.pdf

Notre recherche se situe dans le cadre des PME. Alors, pourquoi les PME représentent-elles un champ d'étude important ? Premièrement, dans la dernière enquête du Clusif (2018), il est prouvé que la maturité des grandes entreprises en matière de sécurité de l'information est plus développée que celle des PME. Et selon Ponemon[4] (2017), plus de la moitié des petites entreprises ont été victimes de cyberattaques et 62% des attaques visaient spécifiquement les petites entreprises. Deuxièmement, car peu de travaux ont étudié la sécurité des SI dans les PME (Kyobe, 2008, Barlette et al, 2017), et pourtant elles sont aussi et de plus en plus concernées par des risques en matière de système d'information.

Dans cette optique notre objectif de recherche est de déterminer comment évaluer la maturité de la culture sécurité SI dans les PME ?

Nous allons tout d'abord définir ce qu'est une culture sécurité dans le champ des SI et la caractériser notamment en explorant ces facteurs déterminants et les relations entre ces facteurs pour ensuite définir notre modèle théorique et enfin présenter notre méthode de recherche qui permettra de valider ce modèle pour les PME.

2. La culture sécurité des SI :

Plusieurs auteurs ont tenté de définir le concept de la culture sécurité de l'information, c'est le cas de 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* ''.

Une autre définition est celle proposée par Schlienger et Teufel, (2003) : « *La culture de 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 des activités quotidiennes de chaque employé* ». Pour Dhillon (1997) il définit que la culture de sécurité est le comportement dans une organisation qui contribue à la protection des données, des informations et des connaissances.

Selon (Ngo, Zhou, et Warren, 2005) la culture de la sécurité de l'information est souvent expliquée à l'aide d'une variété de théories et de principes établis issus d'autres domaines de recherche. En effet, la culture de la sécurité de l'information est un domaine de recherche nouveau et émergent. Il est donc logique d'utiliser d'autres théories comme base de recherche.

La plupart des auteurs, qui ont tenté à définir le concept de la CSI se sont donc basés sur la culture organisationnelle. Selon Schlienger et Teufel (2003) et Van Niekerk et Von Solms (2005), la culture de la sécurité de l'information est une sous-culture de la culture organisationnelle. Ils font référence aux comportements dans une organisation lorsque les employés traitent les informations.

À son tour la sous-culture est un sous-système qui a des valeurs, des normes et des connaissances spécifiques qui la différencient de la culture organisationnelle.

La définition que donne E. Schein (1990) de la culture organisationnelle est la suivante : « *La culture peut être définie comme un ensemble d'hypothèses fondamentales qu'un groupe donné a inventé, découvert ou constitué en apprenant à résoudre ses problèmes d'adaptation externe et d'intégration interne. Ces hypothèses ont été suffisamment confirmées dans l'action de sorte qu'on puisse les*

[4]https://csrps.com/Media/Default/2017%20Reports/2017-Ponemon-State-of-Cybersecurity-in-Small-and-Medium-Sized-Businesses-SMB.pdf

considérer comme valides, et donc les enseigner à tout nouveau membre du groupe, en les présentant comme la manière appropriée de pouvoir, penser et sentir les problèmes de l'action collective ».

Initiant ce qui va fonder le raisonnement en « couches », raisonnement très souvent utilisé en management interculturel, E. Schein 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 (2003) présentent les trois niveaux de la culture sécurité de l'information. Ces niveaux et leurs interactions sont représentés dans le schéma suivant :

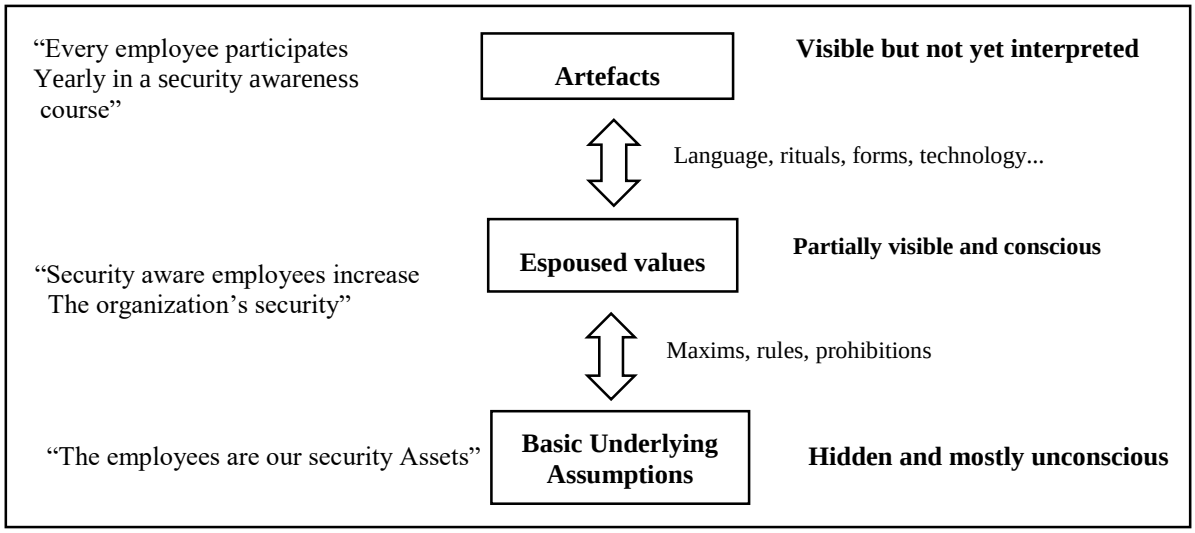

Figure 2 : Les trois niveaux de la culture sécurité de Schlienger et Teufel (2003) adapté de (Schein 1985)

Donc, en se référant à Schein et son modèle des trois niveaux de culture nous déduisons 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. Ces trois niveaux se présentent 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 bases 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 (Schlienger et Teufel, 2003).

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. 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 sécurité de l'information devient un aspect naturel dans les activités quotidiennes de chaque employé. (Schlienger et Teufel, 2003).

L'instauration d'une culture de la sécurité nécessitera à la fois une impulsion et une large participation et devrait se traduire par une priorité renforcée donnée à la planification et la gestion de la sécurité, ainsi que par une compréhension de l'exigence de sécurité par l'ensemble des participants. Les questions de sécurité doivent être un sujet de préoccupation et de responsabilité à tous les niveaux du gouvernement et des entreprises et pour l'ensemble des parties prenantes. (OCDE[5], 2002).

Les chercheurs ont précédemment proposé des divers cadres conceptuels pour la gestion de la sécurité de l'information qui inclure le développement culturel de la sécurité de l'information basé sur les initiatives de gestion de la politique, sensibilisation, formation et éducation (Knapp et al, 2006). Ces dernières années, plusieurs modèles traitant la culture de la sécurité de l'information ont émergé, basés sur la culture organisationnelle et mesure la culture de la sécurité de l'information (Schlienger et Teufel, 2003); valeurs partagées (Helokunnas et Iivonen, 2003), la sensibilisation à la sécurité de l'information (von Solms, 2000); contributions associé au développement de niveaux individuels, de groupe et organisationnels de sécurité de l'information l'enculturation (Martins et Eloff, 2001); perspective socio-technique de la sécurité de l'information (Stanton et Al, 2004); approche persuasive de sensibilisation prescriptive basée sur la morale et l'éthique (Siponen, 2000); méthodes informelles d'enculturation (Vroom et von Solms, 2004); concepts clés de la culture organisationnelle (Zakaria et Gani, 2003); capacités du personnel (Furnell et Clarke, 2005); apprentissage organisationnel (van Niekerk et von Solms, 2003) et une approche multiforme (Chia et al, 2002).

Si ces cadres sont clairement utiles, ils représentent un champ théorique centré sur les grandes organisations. En outre, ils ne traitent pas les défis de sécurité de l'information rencontrés par les PME. Nous allons présenter dans la partie suivante les composants qui constituent et les composants qui influencent la culture sécurité tels que présentés dans la littérature, en mettant l'accent sur les composants qui intéressent surtout les PME.

3. Facteurs qui constituent et facteurs qui influencent la culture sécurité :

Lors de notre revue de littérature sur la culture sécurité de l'information, 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. Nous allons présenter tout d'abord les facteurs qui constituent la CSI ensuite nous allons présenter et classer ces facteurs qui influencent la CSI en facteurs endogènes et facteurs exogènes et enfin nous intègrerons un facteur important de la PME qui est la direction et principalement son dirigeant.

5 Organisation De Coopération Et De Développement Économiques.

En effet dans la PME les fonctions sont intégrées et le dirigeant en contrôle tous les aspects en dirigeant plusieurs fonctions et même en y participant (Torres, 1998).

3.1 Facteurs qui constituent la CSI :

-Conscience de sécurité : défini lorsque les utilisateurs comprennent les problèmes potentiels liés à la sécurité de l'information 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).

-Propriété de sécurité (Responsabilité) : 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). Les parties prenantes dont les utilisateurs doivent comprendre leur responsabilité dans la sécurité des systèmes et réseaux et en être, en fonction du rôle qui est le leur, individuellement comptables. (OCDE, 2002).

-Conformité à la sécurité : conformité du comportement des employés avec la politique, les réglementations et les pratiques de sécurité afin de réduire les atteintes à la sécurité causées par un comportement inadéquat des employés et d'améliorer la culture de sécurité des informations au sein des organisations (Da Veiga et Martins, 2017).

Si nous revenons à la théorie des trois niveaux de la culture sécurité de Schlienger et Teufel (2003), nous trouvons que chaque facteur qui constitue la culture sécurité correspond à un niveau de la culture sécurité. D'où la conscience de sécurité correspond aux hypothèses de bases, la propriété de sécurité correspond aux valeurs partagées et enfin la conformité à la sécurité qui correspond aux artefacts.

3.2 Facteurs qui influencent la CSI :

Nous avons classé les facteurs qui influencent la CSI en trois catégories, la première regroupe les facteurs endogènes, la deuxième catégorie pour les facteurs exogènes et la troisième concerne la direction et plus particulièrement la sensibilité du dirigeant à la sécurité.

3.2.1 Facteurs endogènes :

-Formation à la sécurité de l'information : est un processus d'apprentissage qui fournit une connaissance générale d'un certain sujet lié à l'environnement de sécurité et les compétences de sécurité requises pour que les employés puissent exécuter les procédures de sécurité (Da Veiga et Martins, 2017), (Knapp et al, 2006).

-Evaluation des risques : 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 sécurité de l'information (Da Veiga et Eloff, 2010 ; Martins et Eloff, 2002).

3.2.2 Facteurs exogènes :

-Contexte réglementaire **:** les gouvernements peuvent jouer des rôles de soutien clés. La distribution de brochures de sensibilisation à la sécurité de l'information aux PME et la conduite de l'analyse comparative nationale de la sécurité de l'information des PME. Pour aider les organisations, des exemples de scénarios de risque de sécurité peuvent être développés à partir des ressources de sécurité existantes. (Dojkovski et al, 2007).

-Prestataire de services : les fournisseurs de technologies de sécurité de l'information jouent des rôles clés. Ils peuvent fournir une sensibilisation à la sécurité de l'information, mais ils peuvent également fournir une fiabilité aux PME qui, autrement, pourraient se sentir vendues du matériel et des logiciels inutiles. (Dojkovski et al, 2007).

3.2.3 Direction :

-Sensibilité du dirigeant à la sécurité : se réfère à un degré de la compréhension par la haute direction de l'importance de la fonction de sécurité de l'information et participe aux activités de sécurité visant à améliorer et à créer une forte culture de la sécurité de l'information (Martin et Da Veiga, 2015).

Ces constructions semblent être les facteurs les plus influents et sont considérées comme faisant partie de la conceptualisation de la culture de la sécurité de l'information. Dans le cadre d'études, il existe une distinction claire entre les facteurs qui constituent et les facteurs qui influencent la culture de la sécurité de l'information**.**

4. Propositions et modèle de recherche :

4.1 Propositions de la recherche :

À partir de la revue de littérature sur les composants et les facteurs qui influencent la culture sécurité de l'information, nous avons pu fonder nos propositions de recherche qui dictent notre modèle théorique. Nous nous présentant tout d'abord nos quatre propositions et les sous-propositions qui en découlent.

Proposition 1 : 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.

P1a : Le **contexte règlementaire et légal** 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. À titre d'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. Il renforce et unifie la protection des données pour les individus au sein de l'Union européenne. Et elle oblige à terme les entreprises à mettre

en place des procédures spécifiques, et accroissant le montant des amendes jusqu'à 1 million d'euros. Ce règlement est entré en application le 25 mai 2018. 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 ou PME moins sensibles à la sécurité des SI que les grands groupes. Autre exemple, la charte de cybersécurité mise en place par la CCI qui s'inscrit dans une démarche destinée à réduire les risques numériques tant au niveau des prestataires que de leurs clients. À notre avis cette influence n'est pas encore testée dans les études qui portent sur la culture sécurité de l'information, mais dans les 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.

P1b : Prestataire des services informatiques et numériques : peut jouer un rôle clé dans la sensibilisation à la Sécurité des SI, mais aussi peuvent 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. Cette influence, a été testée dans des PME australiennes par Dojkovski et al (2007).

P1c : Secteur d'activité : Nous distinguons ici les PME techniques (appartenant aux secteurs de : l'informatique, Télécommunications, service financier…) des PME non techniques (appartenant aux autres secteurs d'activité), ces dernières peuvent avoir des problèmes plus graves. 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. À notre connaissance, aucune des études antérieures n'a testé l'influence directe du secteur d'activité dans le domaine de la Culture sécurité de l'information. Seule, une étude de Dagorn et Poussing (2012), en matière de gouvernance de la sécurité de l'information, montre la difficulté à traduire les concepts en actions concrètes, appartenir au secteur de l'industrie comparativement au secteur des services. Nous avons identifié d'autres études où les auteurs soulignent l'importance qui peut avoir l'effet de l'activité de l'entreprise dans ce domaine. Djokovski et al (2007), Barlette (2012).

Proposition 2 : Des facteurs endogènes comme l'existence d'une évaluation des risques sécurité des SI ou la réalisation de formations en matière de sécurité des SI influencent positivement la culture sécurité SI de la PME.

P2a : La **gestion des risques,** par l'intermédiaire d'une analyse et une évaluation des risques, peut contribuer à une meilleure culture sécurité des SI au sein des PME. Djokovski et al (2007) ont montré 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 sécurité de l'information. (Etude sur des PME australiennes). De plus 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.

P2b : Une **formation** à la sécurité pour les employés aura une influence positive sur leur culture sécurité. (Djokovski et Al, 2007 ; Alnatheer, 2012 ; Da Veiga, 2015). 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).

Proposition 3 : La direction de la PME joue un rôle important dans la création d'une culture sécurité SI.

Le **Support de la direction/Leadership :** plus la direction est impliquée dans la gestion de la sécurité des SI, plus le niveau de la culture sécurité des SI au sein de la PME sera important. Il était démontré que les dirigeants de PME jouent 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). 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 souvent pas 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, tels 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).

Proposition 4 : L'adoption d'une culture sécurité est favorable à créer un comportement sécuritaire.

Une étude de Parsons et al (2015), montre que la culture sécurité de l'information 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 culture sécurité de l'information et le comportement en matière de sécurité. Bien qu'ils ne se soient pas concentrés uniquement sur l'effet du concept de la culture sécurité de l'information 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.

Cette connaissance est cruciale pour permettre une compréhension complète de l'influence de la culture sécurité sur le comportement en matière de sécurité, en particulier dans le contexte de la théorie du comportement planifié (TPB). Une autre étude plus récente de Conolly et Al (2017) montrent 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 sécurité de l'information. Cette prise de conscience, à son tour, tend à empêcher les actions

malveillantes des employés et encourage les comportements sécuritaires. Cette influence n'est pas encore étudiée au niveau des PME.

4.2 Modèle de la recherche :

À partir des 4 propositions de recherche issues de la revue de littérature et les sous-propositions qui en découlent nous avons pu construire notre modèle de recherche présenté dans la figure 1 et qui montre l'interaction de la culture sécurité avec les facteurs exogènes, les facteurs endogènes et la direction et qui favorise ensuite la création d'un comportement sécuritaire.

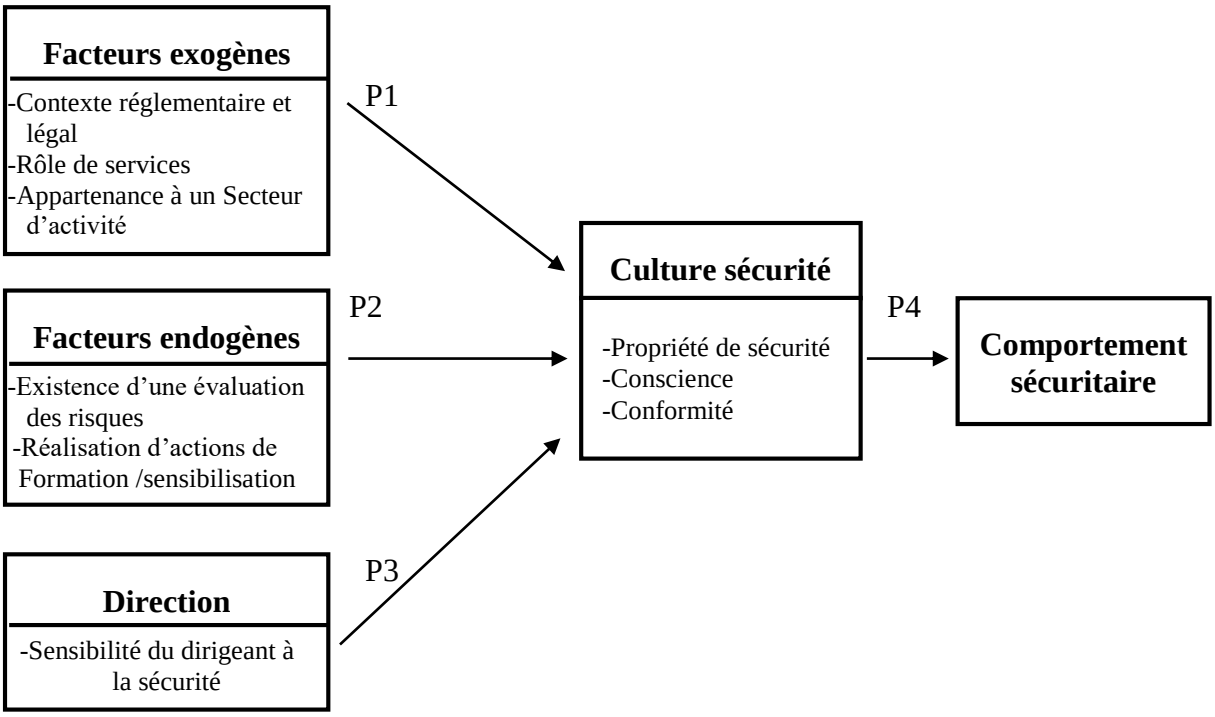

Figure 1 : Modèle théorique de la recherche

5. Méthode de recherche :

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. 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. Nous sommes à un stade exploratoire et nous désirons expliquer un phénomène social. Nous réaliserons donc une étude de cas multiples qui se fera sous forme d'entretiens semi-directifs.

Nous avons évoqué en introduction les problèmes des PME en matière de sécurité des SI, pour cela nous avons ciblé les entreprises de moins de 250 personnes tous secteurs d'activité confondus. Nous avons contacté des dirigeants de PME de la région Ouest sans avoir une vision préalable sur leur sensibilité à la sécurité des Systèmes d'information.

Nous avons commencé à contacter les PME par emails et/ou des appels téléphoniques à partir de contact obtenu par le réseau de la CCI[6] métropolitaine. Nous avons déjà reçu 8 réponses favorables (Voir liste des entreprises et leurs caractéristiques en Annexe 1). L'entretien dure de 15 à 60 minutes selon le type de public à partir d'un guide d'entretien (Voir annexe 2 et 3) que nous avons élaboré à partir de notre grille de recherche. Les guides d'entretien sont adaptés à chaque type d'acteur interrogé. Ils sont composés des thèmes tirés de notre modèle théorique, chaque thème regroupe un nombre de questions précises destinées à approfondir notre compréhension sur les points d'investigation. Chaque entretien est enregistré après avoir la permission de chaque acteur interrogé. Nous avons rencontré les dirigeants et/ou les principaux responsables de la PME dans un premier temps 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.

6. Conclusion :

Nous avons donc élaboré notre modèle de recherche qui va nous permettre ensuite d'évaluer la maturité de la culture sécurité des SI dans les PME. À ce jour, nous avons effectué 15 entretiens semi-directifs dans 4 PME avec les dirigeants, les responsables et les salariés, d'autres entretiens sont en cours de réalisation et leur analyse sera effectuée une fois toutes les études de cas seront finalisés. L'analyse de ces entretiens peut nous aider à identifier d'autres facteurs qui pourraient émerger. Notre objectif est d'atteindre un nombre de 10 à 12 études de cas ce qui devrait garantir un degré de certitude, et d'obtenir une saturation théorique satisfaisante (Yin, 1989 ; Thiétart, 1999).

Les limites d'une telle étude seraient principalement liées au nombre de cas, à la difficulté de prise en compte de certaines variables telles que l'expérience des acteurs. Comme pour beaucoup d'études de ce type, il sera nécessaire d'étudier les contraintes liées à sa généralisation.

Une étude quantitative complémentaire sera intéressante pour généraliser notre étude et vérifier la validité du modèle théorique. Enfin, d'autres recherches serviront à établir des procédures et des méthodes afin de guider les managers dans les actions à mettre en place pour insuffler une culture sécurité des SI dans les PME. Concernant les utilisateurs, des chartes d'utilisation ou des guides de bonnes pratiques pourront être mises en place, ainsi que des formations à la sécurité des SI. Les pistes de recherche sont nombreuses, et leurs résultats permettront de faire progresser la culture sécurité dans les PME. Dans un cadre plus général, mieux diffuser une culture sécurité des informations pourra aboutir à une meilleure protection des actifs informationnels des PME et de renforcer leurs performances.

[6] CCI : Chambre de Commerce et de l'Industrie

Références

Alnatheer AM., Chan T., Nelson K. (2012), Understanding and Measuring Information security Culture, *Pacific Asia Conference on Information Systems, PACIS 2012 Proceedings.*

Alnatheer AM. (2014), A conceptual model to understand information security culture, *International Journal of Social Science and Humanity*, Vol. 4, No. 2, March 2014.

Barlette Y., Jaouen A. (2019), Information security in SMEs: determinants of CEOs' protective and supportive behaviors, *Systèmes d'information et management,* N° 3 – VOL. 24 – 2019.

Barlette Y., Gundolf K., Jaouen A. (2017). CEO's information security behavior in SME's: Does ownership matter? *Systèmes d'information et management,* 2017, 3 V-22.

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

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.

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, doi: 10.1108/ICS-03-2017-0013.

CLUSIF (2018), *Menaces informatiques et pratiques de sécurité en France*, Edition 2018.

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

Chia PA., Maynard S B., Ruighaver A B. (2002), Exploring Organisational Security Culture: Developing A Comprehensive Research Model, *in Proceedings of IS ONE World Conference, Las Vegas.*

Dagorn N., Poussing N. (2012), Engagement et pratiques des organisations en matière de gouvernance de la sécurité de l'information, *Systèmes d'information et management*, Vol17, p.113-143.

Da Veiga A., Eloff J H P. (2010), A framework and assessment instrument for information security culture, *Computers and Security*, Vol. 29 No. 2010, pp. 196–207.

Da Veiga A., Martins N. (2017), Defining and identifying dominant information security cultures and subcultures, *Computers and Security* (2017).

De Guinea A O., Kelley H., Hunter M G. (2005), Information Systems Effectiveness in Small Businesses, *Journal of Global Information Management*, vol. 13, n°3, p. 55-79.

Dhillon G. (1997). *Managing Information System Security*, MacMillan Press Ltd, Great Britain.

Dojkovski S. (2007), Fostering information security culture in small and medium size entreprises: An interpretive study in Australia'', *European Conference on Information Systems (ECIS).120.*

Dutta A., McCrohan K. (2002), Management's Role in Information Security in a Cyber Economy, *California Management Review*, 45(1), fall, 67-87.

Ernst et Young (2006), 2006 Global Information Security Survey, *Ernst and Young*.

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.

Furnell S M., Clarke N L. (2005), Organizational Security Culture: Embedding Security Awareness, Education and Training, *in Proceedings of the 4th World Conference on Information Security Education (WISE 2005), Moscow, 67-74.*

Hassan N H., Ismail Z. (2012), A conceptual model for investigating factors influencing information security culture in healthcare environment, *Procedia - Social and Behavioral Sciences* 65 (2012) 1007 – 1012.

Helokunnas T., et Iivonen I. (2003), Information Security Culture in Small and Medium Size Enterprises, *Seminar Presentation, Institute of Business Information Management, Tampere University of Technology, Finland.*

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

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.

Kotulic A., Clark J G. (2004), Why there aren't more information security research studies, *Information and Management*, (41:5), pp. 597-607.

Knapp KJ., Marshall T E., Rainer R K., Ford F N. (2006) Information Security: Management's effect on culture and policy, *Information Management and Computer Security*, 14(1), p.24-36.

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.

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

Martins A., Eloff J. (2002), Assessing Information Security Culture, *Information for Security 2nd Annual Conference, South Africa.*

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.*

Martins N., Da Veiga A. (2015), An Information Security Culture Model Validated with Structural Equation Modelling, *Proceedings of the Ninth International Symposium on Human Aspects of Information Security and Assurance (HAISA 2015).*

Niekerk J., Solms R. (2005), A holistic framework for the fostering of an information security sub-culture in organizations, *The Information Security Conference proceedings, Johannesburg, South Africa.*

Van Niekerk J C., von Solms R. (2003), Establishing an Information Security Culture in Organizations: an Outcomes-based Education Approach, *in Proceedings of ISSA 2003:3rd Annual IS South Africa Conference, Johannesburg, South Africa, 9-11 July 2003.*

Ngo L., Zhou W., Warren M. (2005), Understanding Transition towards Information Security Culture Change, *Proceedings of the 3rd Australian Information Security Management Conference*, Perth, *Western Australia.*

OECD (2002), OECD Guidelines for the Security of Information Systems and Networks: TOWARDS A CULTURE OF SECURITY, *1037ème session, 25 juillet 2002.*

Parsons K M., Young E., Butavicius MA., McCormac A. (2015), The Influence of Organizational Information Security Culture on Information Security Decision Making, *Journal of Cognitive Engineering and Decision Making*, 2015, Volume 9, Number 2, June 2015, pp. 117-129.

Schein E H. (1990), Organizational Culture, *American Psychologist*, vol. 45, n° 2, 1990, pp. 109-119.

Schein E H. (1985), *Organizational culture and leadership*, San Francisco: Jossey-Bass Publishers, 1985, 358 p.

Schlienger T., Teufel S. (2003), Information security culture: from analysis to change, *South African Computer Journal*, Vol. 31, p. 46-52.

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.

Stanton J M., Stam K R., Mastrangelo P R., Jolton J. (2004) Analysis of end-user security

behaviors, *Computers and Security*, 24, p. 124-133.

Tolah A., Furnell S M., Papadaki M. (2017), A Comprehensive Framework for Cultivating and Assessing Information Security Culture, *Proceedings of the Eleventh International Symposium on Human Aspects of Information Security and Assurance, University of Plymouth, Royaume-Uni.*

Torrès O. (1998), *PME : de nouvelles approches*, Editions Economica, Collection Recherche en Gestion.

Thomson K., von Solms R., Louw L. (2006), Cultivating an Organizational Information Security Culture, *Computer Fraud and Security*, 2006(10), p.7-11.

Thiétart R A. (1999), *Méthodes de recherche en management, Dunod*, Paris.

Von Solms B. (2000) Information Security - The Third Wave?, *Computers and Security*, 19(7), 615-620.

Vroom C., von Solms R. (2004), Towards information security behavioural compliance, *Computers and Security*, 23(3), p. 191-198.

Galletta D F., Polak P. (2003), An Empirical Investigation of Antecedents of Internet Abuse in the Workplace, *AIS SIG-HCI Workshop, Seattle, December, 2003*.

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.

Wang J., Gupta M., Rao H R. (2015), Insider Threats in a Financial Institution: Analysis of Attack-Proneness of Information Systems Applications, *Management Information Systems Quarterly*, Vol. 39, n° 1, p. 91-112.

Willison R., Warkentin M. (2013), Beyond Deterrence: An Expanded View of Employee Computer Abuse, *MIS Quarterly*, Vol. 37, n°1, p. 1-20.

Yin R K. (1994), *Case study research: Design and methods Second*, Sage Publications.

Yin R K. (1989), *Case study research: design and methods*, Sage, Londres.

Zakaria O., Gani A. (2003), A Conceptual Checklist of Information Security Culture, in *Proceedings of 2nd European Conference on Information Warfare and Security. University of Reading, UK, 30 June – 1 July 2003.*

Annexes

Annexe 1: Caractéristiques des entreprises

Entreprise	Forme juridique	Taille (Salariés)	Chiffre d'affaire (€)	Secteur d'activité
A	SASU	80	35.074.500	Commerce de gros
B	SARL	35	12.795.200	Commerce de gros
C	SARL	40	500.283	Service d'aménagement paysager
D	SAS	70	20.000.000	Transformation et conservation
E	SARL	19	2 .029.300	Commerce de détail
F	Association	250	13.389.000	Aide par le travail
G	SARL	20	1.011.500	Transformation et conservation de légumes
H	SARL	30	2.138.400	Travaux d'étanchéification

Annexe 2 : Guide d'entretien (direction)

Point de départ de l'entretien :

1- Pouvez-vous vous présenter s'il vous plaît ?
2- Depuis quand êtes-vous dans l'entreprise ?
3- Quel est votre poste ou votre fonction au sein de l'entreprise ?

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- 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 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/Contenu.

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 ?

4- 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 ?

-Efficacité de cette mesure ? (sur les résultats, sur le public cible, amélioration ?)

Thème 3 : Sensibilité du dirigeant à la sécurité :

1- Quand vous entendez '' sécurité des systèmes d'information'' qu'est-ce que cela vous évoque ?
2- Est-ce que ça vous intéresse comme sujet ?
3- Qui est/sont les responsable (s) des mesures sécuritaires ? (en terme de décision)
4- 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 ?
5- Que pensez-vous du rôle qu'exerce la direction pour impliquer les collaborateurs dans le respect de ces mesures ?

Conclusion de l'entretien :
Je vous remercie pour ces éléments de réponses.
-Connaissez-vous d'autres PME qui peuvent être sensibles à la SSI ?

Annexe 3 : Guide d'entretien (Salarié)

Point de départ de l'entretien :

1- Pouvez-vous vous 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 ?

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 -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 :

3-Dans quelle mesure, sentez-vous responsable de la sécurité des SI de votre entreprise ?

4 -Quel est votre rôle en matière de sécurité ? Et qu'est-ce qui vous motive à assurer ce rôle ?

*Si la personne ne mentionne pas sa responsabilité :

5 -Sentez-vous obligé à respecter les mesures sécuritaires mises en place au sein de votre entreprise ?

Pour qu'elle raison ?

6 - 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 ?

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…)

8-Avez-vous déjà entendu parler de l'RGPD (Règlement général sur la protection des données) ? Si oui, qu'en pensez-vous ?

- 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 ?

Conclusion de l'entretien :

Je vous remercie pour ces éléments de réponse.