Université Paris 1 Panthéon - Sorbonne

Mémoire de MASTER M2

SYSTÈMES D'INFORMATION ET DE CONNAISSANCE

sous-parcours **Cybersécurité**

Promotion 2021-2022

« Quels sont les impacts du facteur humain sur la surface d'attaque ?»

RÉDIGÉ ET SOUTENU PAR : **Baptiste POISSON**

DIRECTEUR DE MÉMOIRE : **Miguel LIOTTIER**

DATE DE SOUTENANCE : **24 octobre 2022**

L'UNIVERSITE N'ENTEND DONNER AUCUNE APPROBATION

NI IMPROBATION AUX OPINIONS ÉMISES

DANS CE MÉMOIRE :

CES OPINIONS DOIVENT ETRE CONSIDÉRÉES

COMME PROPRES À LEUR AUTEUR

Je soussignée, Madame Mylène JAROSSAY, maître d'apprentissage de Baptiste POISSON, certifie que le mémoire ne contient pas de données confidentielles du groupe LVMH.

Fait à Paris, le 14 octobre 2022.

Signature :

Remerciements

Avant tout, je tiens à remercier **mes parents** et **mon frère**, mes plus fidèles soutiens.

Également, j'adresse des remerciements particuliers à **Guillaume CONTAT** pour la confiance qu'il m'a accordée et les conseils qu'il m'a apportés, sans lesquels mon parcours serait différent, ainsi qu'à **Steeve DETERVID**, qui m'accompagne depuis bientôt une décennie dans ma réussite scolaire, universitaire et professionnelle.

J'adresse mes remerciements à toute l'équipe cybersécurité du groupe LVMH et plus particulièrement à mon maître d'apprentissage, **Mylène JAROSSAY** pour son accueil et sa bienveillance.

Je tiens également à remercier mon directeur de mémoire, **Miguel LIOTTIER** pour sa patience et ses conseils.

Pour cette année universitaire au sein de l'**Université Panthéon-Sorbonne**, je tiens à remercier :

- Mes camarades : **Anas**, **Andrew**, **Adel**, **Arnav**, **Célina**, **Eva**, **Hajar**, **Jimmy**, **Lamyae, Mohammed**, **Pauline**, **Yoshly**, **Zaineb** et **Zoulikha**, mais plus particulièrement **Inès** et **Sara** que j'ai particulièrement sollicitée pour récupérer les cours manqués, élément indispensable à ma réussite universitaire.
- Des sincères remerciements à l'équipe pédagogique et en particulier à Madame **Selmin NURCAN** et Monsieur **Miguel LIOTTIER** pour l'organisation du Master. Un merci particulier également à Monsieur **Bruno PICHON**, Monsieur **Didier CUMENAL,** Monsieur **Ian KING**, Madame **Chaïmae BAGHDADI** et Monsieur **François ROUSSEL.**

Il est important pour moi de remercier ceux qui m'ont soutenu pendant mes études supérieures qui s'achèvent cette année :

- **Université de Paris : Cyrille COELHO** qui fut mon tuteur de l'Université de Paris, mes camarades **Adame**, **Alexis**, **Arnaud**, **Irvin**, **Laure-Anne** et **Maximilien, Osman SALEM**, enseignant.
- **La Rochelle Université : Michel MÉNARD** et **Mickaël COUSTATY** enseignants, **Alessandro PALOMBA** du relais handicap.
- **IUT d'Amiens : Cyril DROCOURT** enseignant, mes camarades **David**, **Léo**, **Anthony**, **Grégoire, Clément** et **Adham.**

Enfin, mes remerciements vont aussi à ceux qui m'ont formé pendant mes stages et apprentissages : **Guillaume**, **Jean**, **Valérie**, **Sandrine**, **Thiébaut**, **Marina**, **Erwan**, **Olivier**, **Catherine**, **Clément et Mylène**. Je n'oublie pas qu'un jour ce sera à mon tour de transmettre mes connaissances aux plus jeunes.

Introduction

Le nombre de cyberattaques explose et s'accompagne d'une médiatisation qui se faisait rare jusqu'à la pandémie du COVID-19 qui a provoqué cette explosion de cyberattaques. Cela a permis la prise de conscience des particuliers, comme des TPE, PME, ETI, collectivités, grandes entreprises et administrations, sur cette menace qui touche notre société.

Nul n'a envie de subir une attaque dont les conséquences peuvent être désastreuses, avec des pertes financières importantes pouvant pousser jusqu'à la faillite. Malheureusement, il n'existe pas de chiffre officiel en France concernant les faillites suite à une cyberattaque, mais ce chiffre est estimé entre 50% et 80% selon des sources Étatsunienne et Anglaise diffusées dans un rapport du Sénat. Le chiffre de 80% est à prendre avec du recul puisqu'il est issu de l'assurance Hiscox, dont on peut estimer que son intérêt est de gonfler ces chiffres pour créer de la peur impliquant un plus grand nombre de souscriptions à son assurance (Meurant & Cardon, 2021).

Face à ces menaces, cette dernière décennie a vu murir plein de nouvelles solutions sous la forme d'un nouveau marché de services. Ce secteur ne devrait pas cesser de croître dans les années à venir, d'autant plus avec le contexte géopolitique actuel qui fait craindre une multiplication des attaques. Ces nouveaux services sont nombreux : logiciels pour surveiller un parc informatique, audit de sécurité, SOC (Security Operations Center) mutualisé, cyber assurance, etc.

Ce sont essentiellement des réponses techniques qui sont apportées, ou des dédommagements en cas de cyberattaque dans le cas des assurances. Mais l'aspect humain est bien souvent oublié, où seul des prestations de sensibilisation auprès des utilisateurs sont proposées (par exemple une campagne d'hameçonnage).

Ainsi, des solutions pour détecter la surface d'attaque d'une entreprise existent, notamment pour la détection des services exposés publiquement. Ces services, du fait de leur exposition en font des cibles privilégiées, ils sont de fait attaquable même si une attaque ne se traduit pas forcément par un succès si le système cible est bien sécurisé. Cependant, ce que l'on peut nommer la surface d'attaque humaine n'est jamais réellement mesurée, le seul indicateur communément retrouvé étant le nombre de personnes s'étant fait piéger par une campagne d'hameçonnage dans le cadre d'une sensibilisation.

Le mélange de la sphère professionnelle avec la sphère privée lors des différents confinements liés au COVID-19 a bouleversé les habitudes des utilisateurs comme des entreprises, ouvrant de nouvelles portes aux attaquants par le télétravail, notamment par des flux supplémentaires parfois mal sécurisés et par l'utilisation des appareils personnels des utilisateurs.

Ainsi, il devient plus que nécessaire de trouver et définir un indicateur fiable et universel permettant de mesurer l'exposition aux attaques d'un système d'information par le biais de ses utilisateurs. Cet indicateur permettra de mieux cibler les actions à effectuer pour améliorer la sécurité du système d'information, que ce soit par des mesures techniques ou organisationnelles.

Cet enjeu est primordial, il s'agit d'un enjeu technico-socio-économique nécessitant la prise en compte de facteurs très divers et complexes dont ce mémoire se veut être une ébauche à la problématique : « Quels sont les impacts du facteur humain sur la surface d'attaque ? ».

En répondant à cette problématique, nous constatons que les impacts du facteur humain sont très importants sur la surface d'attaque et qu'il est nécessaire de pouvoir estimer cette surface d'attaque. Celle-ci est liée à plusieurs facteurs dont la satisfaction des utilisateurs. Ainsi, même avec toutes les mesures de sécurités techniques, le risque d'attaque reste important si le facteur humain n'est pas pris en compte.

Pour cela, nous établirons un état de l'art, en commençant par la surface d'attaque puis en continuant par le succès des systèmes d'information et de l'intention d'utilisation qui sont deux éléments permettant de trouver une solution adéquate.

Suite à l'état de l'art, la méthodologie pour répondre à la problématique sera développé.

Enfin, les résultats de l'enquête seront analysés et des solutions pour qualifier et quantifier la surface d'attaque seront évoqués.

Table des matières

Liste des Figures

Liste des tableaux

1. État de l'Art

1.1. Surface d'attaque : quantifier et qualifier les risques d'attaques

1.1.1. Quantifier la surface d'attaque : difficilement réalisable en prenant en compte le facteur humain

Pour quantifier la surface d'attaque, il faut d'abord s'intéresser à la définition d'une surface d'attaque. La majeure partie des articles évoquant la surface d'attaque, le font dans le cadre d'une surface d'attaque que je nomme dans ce document « surface d'attaque technique », car il s'agit d'évaluer la surface d'attaque d'une technologie en particulier d'un point de vue technique, tel que pour le SQL (Geneiatakis, 2016), les WebSockets (Ghasemshirazi & Heydarabadi, 2021), ou à une portée plus large sur un système utilisant plusieurs protocoles (Manadhata et al., 2007), etc.

Pour ce qui sera nommé « surface d'attaque humaine » dans ce document, les articles évoquent bien souvent l'impact du facteur humain, mais ne quantifie pas de surface d'attaque – ou – quantifie la surface sur un critère particulier, comme l'exemple de l'hameçonnage qui sera abordé par la suite.

Par ailleurs, il est important de définir ce qu'est le facteur humain, notamment dans le cadre dans ce mémoire. Le facteur humain vise à assurer une interface sûre entre l'homme et les autres composants d'un système en tenant compte des performances humaines. Ici, les erreurs de configuration d'éléments techniques (serveurs, applications, etc.) par des administrateurs ne sont pas considérés dans la catégorie « facteur humain ».

Ainsi, cette question de la surface d'attaque est majoritairement traitée d'un point de vue technique, sur des technologies particulières mais beaucoup moins d'un point de vue humain, où seul l'étude sur l'hameçonnage prédomine. Il n'existe pas de consensus dans la communauté scientifique sur une méthode permettant de calculer la surface d'attaque globale du système d'information d'une entité, que ce soit une administration ou une entreprise.

On retrouve alors une multiplicité de définitions pour le terme surface d'attaque dont une revue systématique fait ressortir que 71% des 644 articles du corpus étudié ne définissent pas ce terme (Theisen et al., 2018) (page 98). Dans ce corpus, 48 définitions différentes ont été identifiées (Theisen et al., 2018)(page 99), ce qui tend à démontrer qu'il n'existe pas non plus de consensus sur la définition de surface d'attaque et qu'elle dépend du contexte dans lequel ce terme est utilisé. C'est bien parce qu'il existe des contextes divers et variés qu'il n'existe actuellement pas de solution permettant de quantifier la surface d'attaque d'un système d'information, puisqu'il s'agit là aussi d'un contexte différent que ceux étudiés dans les articles existants. Cette revue systématique permet de faire émerger six définitions dont celle qui sera utilisée dans ce mémoire : « *La surface d'attaque est l'ensemble des façons possibles pour un attaquant de causer des dommages à un système*. », traduction de l'anglais « *The attack surface is the union of all possible ways an attacker could cause damage to a system.* » (Theisen et al., 2018)(page 99).

À partir de cette définition, nous décomposons cette « *ensemble des façons possibles pour un attaquant de causer des dommages à un système* » en deux catégories qui sont interdépendantes : la surface d'attaque technique et la surface d'attaque humaine.

Ces deux catégories sont interdépendantes du fait que la surface d'attaque technique peut amener à exploiter une vulnérabilité humaine et vice versa. Par exemple un fichier malveillant qui arrive dans une boîte e-mail et qu'il est exécuté par un utilisateur, montre une surface d'attaque technique, celle de l'absence ou d'un loupé d'un système d'analyse des pièces jointes, puis une surface attaque humaine d'un utilisateur qui n'a pas pris le temps de vérifier l'expéditeur et autres informations qui lui auraient permis de considérer le fichier comme suspect.

Un autre exemple pour le cas inverse, celui d'un utilisateur qui trouve une clé USB et qui la branche sur son ordinateur professionnel. La surface d'attaque humaine est représentée par cet utilisateur qui n'applique pas de principe de précaution, comme mettre cette clé USB dans une borne de désinfection des clés USB, puis la surface d'attaque technique par l'absence de mesure ne permettant pas l'exécution automatique d'une clé USB inconnue sans analyser le contenu avant.

Enfin, il est important de préciser que des références connues et reconnues existent pour le calcul de surface d'attaque technique, notamment dans le cadre des applications web avec la « *Attack Surface Analysis Cheat Sheet*¶ » de l'OWASP (*Attack Surface Analysis - OWASP Cheat Sheet Series*, 2022) , organisme notamment connu pour son célèbre « OWASP TOP 10 », qui représente un large consensus sur les dix risques de sécurité les plus critiques pour les applications web.

1.1.2. L'hameçonnage : principal vecteur d'attaque passant par l'humain

1.1.2.1. Définir l'hameçonnage et son impact actuel

Tel qu'énoncé précédemment, le cas de l'hameçonnage est sans nul doute le cas le plus documenté concernant les attaques dont l'humain est le principal vecteur permettant à un attaquant d'atteindre sa cible.

Il convient tout d'abord de définir ce qu'est l'hameçonnage – qui se traduit par phishing en anglais. On trouve premièrement les « définitions » apportées par les autorités publiques françaises, tels que :

- « Le fraudeur se fait passer pour un organisme que vous connaissez (banque, service des impôts, CAF, etc.), en utilisant le logo et le nom de cet organisme. Il vous envoie un mail vous demandant généralement de "mettre à jour" ou de "confirmer vos informations suite à un incident technique", notamment vos coordonnées bancaires (numéro de compte, codes personnels, etc.). » (CNIL, 2022)

- « L'hameçonnage ou *phishing* est un SMS ou mail frauduleux destinés à tromper la victime pour l'inciter à communiquer des données personnelles et/ou bancaires en se faisant passer pour un tiers de confiance. » (Cybermalveillance, 2022)

- « L'hameçonnage reste l'un des principaux vecteurs de la cybercriminalité. Ce type d'attaque vise à obtenir du destinataire d'un courriel d'apparence légitime qu'il transmette ses coordonnées bancaires ou ses identifiants de connexion à des services financiers, afin de lui dérober de l'argent. L'hameçonnage peut également être utilisé dans des attaques plus ciblées pour essayer d'obtenir d'un employé ses identifiants d'accès aux réseaux professionnels auxquels il peut avoir accès. » (ANSSI, 2022)

Il existe aussi des associations qui définissent ce terme comme :

- « Technique d'attaque informatique reposant sur l'ingénierie sociale et utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La méthode consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. — afin de lui soutirer les renseignements demandés. » (CLUSIF, 2022)

En France, 73% des entreprises déclarent l'hameçonnage comme vecteur d'entré principal pour les attaques subies d'après la 7ème édition du baromètre annuel du CESIN. (CESIN, 2022)

Enfin, « L'hameçonnage est un acte de tromperie évolutif par lequel l'usurpation d'identité est utilisée pour obtenir des informations d'une cible », de l'anglais « *Phishing is a scalable act of deception whereby impersonation is used to obtain information from a target* » d'après une revue systématique sur 526 articles gardés permettant d'obtenir une définition consensuelle issue la communauté scientifique (Lastdrager, 2014).

1.1.2.2. Étude sur le sujet du phishing en prenant en compte le facteur technique

Les études sur l'hameçonnage sont très intéressantes car ces études révèlent la complexité et le nombre de domaines qui interagissent dans l'aboutissement des attaques de cette nature.

Ainsi, on retrouve un modèle composé de trois couches qui sont le support, le vecteur et l'approche technique (Chiew et al., 2018).

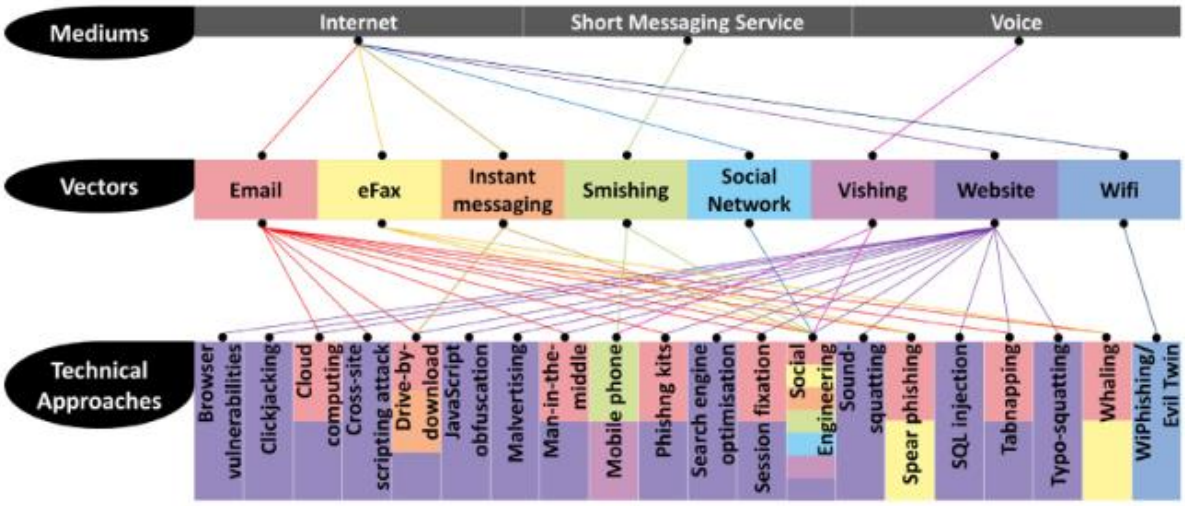

Figure 1 : Les liens entre les différentes couches (Chiew et al., 2018)

Le modèle illustré dans la *Figure 1* est intéressant surtout pour les couches « vecteurs » (*Vectors)* et « approches techniques » (*Technical Approches)*. Cependant, la catégorie « supports » (*Mediums*) ne semble pas être d'un grand intérêt puisqu'il est tout à fait possible de faire de l' « hameçonnage par téléphone » (*Vishing)* et de l' « hameçonnage par SMS » (*Smishing)* par Internet notamment par l'utilisation de SMS par Internet qui permet d'être d'autant plus crédible pour faire du « hameçonnage par SMS » (*Smishing)* car l'utilisation d'un numéro de téléphone « lambda » serait plus suspect. Ainsi, dans cette figure, ce sont les différentes catégories de la couche approches techniques et de la couche vecteurs qui sont particulièrement intéressantes plus que les liens qui là aussi sont critiquables.

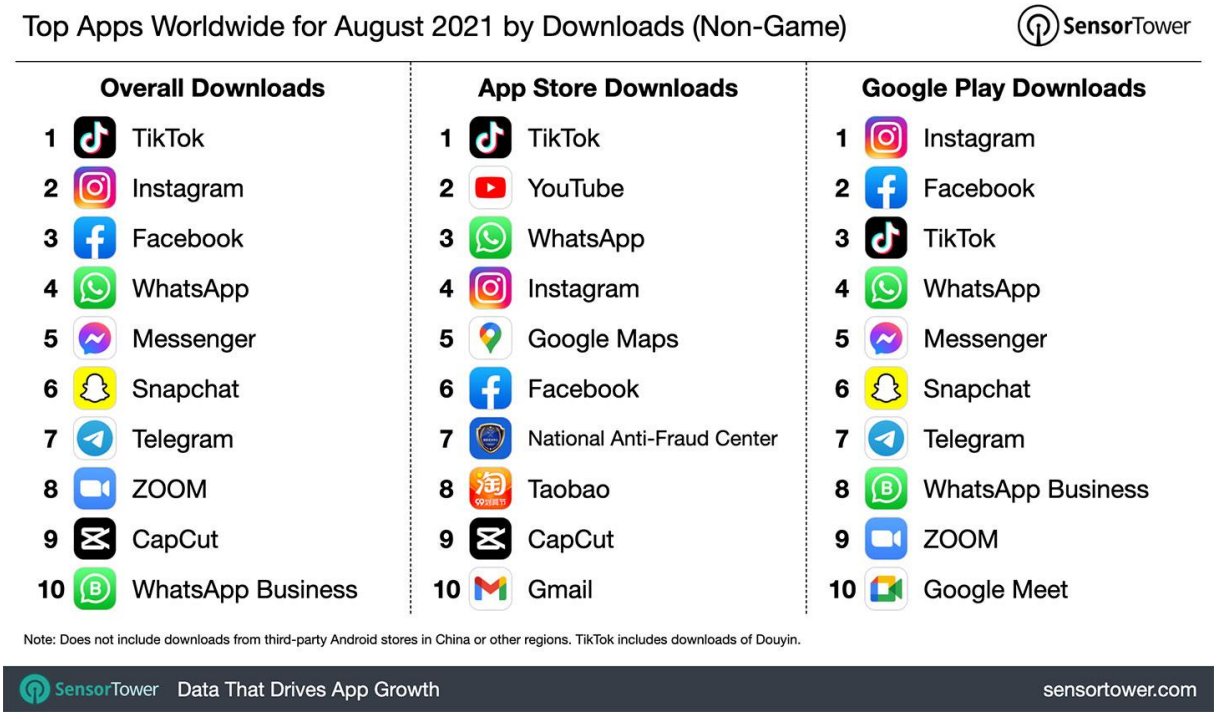

Figure 2 : Applications les plus téléchargés à travers le monde. Source : sensortower.com

En effet, aujourd'hui les smartphones permettent bien plus que d'être uniquement la cible de *Smishing* et de *Vishing*, notamment par l'utilisation de messageries instantanées, la consultation de courriels, de sites web, comme le montre la *Figure 2*, bien qu'il s'agisse du nombre de téléchargement donc que cela ne reflète pas l'utilisation des applications déjà installées (application d'email, de sms, navigateur, etc).

En dehors de cette étude prenant largement en compte les enjeux techniques derrière l'hameçonnage, de nombreuses autres études évoquent les aspects démographiques, psycho-sociaux et le contexte.

1.1.2.3. L'impact du genre

Cette partie ainsi que les suivantes sont en partie issue des résultats d'une étude qui se nomme « *Experimental Investigation of Technical and Human Factors Related to Phishing Susceptibility* » (Greitzer et al., 2021) et qui elle-même reprend les résultats de nombreuses études.

Dans les études sur l'hameçonnage, on retrouve des éléments contradictoires sur les publiques les plus susceptibles d'être victime d'hameçonnage. Notamment, on retrouve quartes études concluant que les femmes sont plus susceptibles d'être victime d'hameçonnage contre deux études affirmant qu'il n'y a pas de différence entre les sexes. Cependant, cette information permet certes de mieux cibler une catégorie de personne mais pas d'en comprendre les mécanismes poussant certaines personnes à se faire hameçonner. Cependant, ces études ne sont pas axées sur des différences biologiques, ce qui ne permet pas d'affirmer que c'est uniquement le sexe de la personne qui définit sa susceptibilité à être hameçonné du fait de facteurs biologiques. Ainsi, il est nécessaire de comprendre les mécanismes sous-jacents afin d'être en mesure d'enrayer le problème au-delà du sexe de la victime.

Dans le détail, la première étude donnant pour résultat que les femmes sont plus susceptibles de se faire avoir par du phishing montre que 77% des femmes se font avoir contre 65% pour les hommes (Jagatic et al., 2007). Cependant, les hommes se font avoir à 68% quand le phishing laisse apparaître que l'expéditeur est une femme contre 53% lorsque l'expéditeur est un homme. Alors que la variation observée pour les femmes est moindre, avec 78% quand l'expéditeur est un homme contre 76% lorsque l'expéditeur est du même sexe (Jagatic et al., 2007). Malheureusement, bien que ce résultat soit intéressant, aucune n'explication n'est donnée mais ce constat doit nous amener à réfléchir sur les conclusions et les mesures à en tirer.

Un autre article met en perspective un élément particulièrement intéressant qui est celui de l'éducation contre l'hameçonnage. Cinq groupes différents ont été exposés à différentes formations (ou absence de formation) sur l'hameçonnage dont :

- L'absence de formation
- Une sensibilisation basée sur les trois premiers résultats google de la recherche « phishing »

- Une sensibilisation basée sur le jeu vidéo « Anti-phishing phill » (Sheng et al., 2007)
- Une sensibilisation basée sur la BD « PhishGuru »
- Une sensibilisation avec à la fois le jeu vidéo « Anti-phishing phill » et la BD « PhishGuru »

Le résultat montre que la sensibilisation a un impact significatif, provoquant une amélioration de l'ordre de 40%. Cependant, cette étude montre que les femmes restent plus susceptibles d'être hameçonnées, 54,7% des femmes ayant cliqué sur un lien d'hameçonnage contre 49% pour les hommes. Ce résultat reste néanmoins nuancé par l'hypothèse que les victimes femmes avaient moins de compétences techniques que les hommes lors de cette étude (Li et al., 2020).

Concernant les deux autres études montrant que les femmes sont plus susceptibles que les hommes à se faire hameçonner, on retrouve les chiffres suivants :

- 53% des femmes se sont fait hameçonner contre 14% pour les hommes (Halevi et al., 2013).
- Pour la détection d'un courriel d'hameçonnage en analysant l'en-tête et le corps du courriel, 59,3% des courriels légitimes sont considérés comme de l'hameçonnage par les femmes, contre 54,3% des hommes. Et 36,8% des courriels d'hameçonnages sont considérés comme légitimes par femmes contre 20,7% pour les hommes. Les chiffres ont été mis en pourcentage pour la comparaison mais sont présentés comme un indice de précision sur 10 dans l'étude initiale (Blythe et al., 2011).

Pour ce qui est des études montrant aucun changement significatif on trouve :

- 22,8% des hommes contre 20.9% des femmes ont cliqué sur des liens de phishings
    - L'étude semble cependant comporter une coquille puisqu'il est mentionné : « *Among the clickers, we observed that males are more likely to click on the credit card email than females*. » alors que la figure 4 de cette étude montre le contraire lors de la répartition des clics selon le type de phishing, laissant planner un doute sur quelle information est la bonne (Li et al., 2020)
- 71,38% des hommes ont cliqué sur le lien de phishing contre 68,54% des femmes (Diaz et al., 2018).

Ces multiples études montrent bien l'absence de consensus sur l'impact du genre et la susceptibilité de se faire hameçonner. Cependant, nous verrons par la suite que ces résultats peuvent s'expliquer par les traits de personnalités.

1.1.2.4. L'âge : une fiabilité court terme

Outre le facteur genre qui a été détaillé ci-dessus et qui ne permet pas de tirer de conclusion sur les personnes susceptibles de se faire hameçonner et donc augmentant la surface d'attaque, le facteur de l'âge a lui aussi été étudié avec des résultats

contradictoires. En effet, trois cas de figures apparaissent et avec pour chacun deux études allant dans leur sens :

- Les personnes âgées de plus de 59 ans sont plus susceptibles d'être victime d'hameçonnage que le reste de la population (Li et al., 2020; Lin et al., 2019).
- Les personnes âgées de 18 à 24 ans sont plus vulnérables au phishing (Jagatic et al., 2007; Sheng et al., 2010).
- Aucune différence entre les populations (Downs et al., 2006; Mohebzada et al., 2012)

Malgré des études contradictoires, ces études laissent penser que les populations les plus susceptibles de se faire hameçonner sont les plus jeunes et les plus âgés, dans le premier cas à cause d'une potentielle immaturité avec l'outil numérique et dans le second cas parce que ce sont des personnes n'ayant pas connu l'outil informatique dès leur jeune âge comme c'est le cas aujourd'hui. Cependant la fragilité de ces études réside dans le temps, c'est-à-dire que ceux qui seront dans la catégorie des plus de 59 ans dans dix ans ne refléterons pas les constats d'il y a deux à seize ans.

Ces résultats montrent cependant que les plus jeunes, qui ont grandi avec les outils numériques, ne sont pas forcément plus vigilants sur les risques qui en sont liés. Ainsi, comme il existe une éducation civique dans le système éducatif français, une éducation aux outils numériques et leurs risques pourraient réduire ces risques aussi bien dans la vie quotidienne de la population qu'en entreprise.

1.1.2.5. Les facteurs psychosociaux

Les facteurs psychosociaux sont plus difficiles à cerner que l'âge et le genre, ce qui nécessite d'avoir des critères permettant de qualifier les personnes. Pour cela il existe notamment « The Five-Factor Theory of Personality » (McCrae & Costa, 2008) qui définit cinq grands profils (Tableau 1).

Dimension de la personnalité	Tendance (abstrait)	Caractéristiques (concret)
Névrotisme (*Neuroticism*)	Dépression (tendance à éprouver des affects dysphoriques - sentiment de détresse, de désespoir, de culpabilité).	Faible estime de soi, croyances perfectionnistes irrationnelles, attitudes pessimistes.
Extraversion	Grégaire (préférence pour la compagnie et la stimulation sociale).	Compétences sociales, nombreuses amitiés, intérêts professionnels entreprenants, participation à des sports d'équipe, adhésion à des clubs.
Ouverture à l'expérience (*Openness to experience*)	Actions (besoin de variété, de nouveauté et de changement).	Intérêt pour les voyages, nombreux passe-temps différents, connaissance de la cuisine étrangère, intérêts professionnels variés, amis partageant les mêmes goûts.
Amabilité (*Agreeableness*)	Conformiste (volonté de s'en remettre aux autres en cas de conflit interpersonnel).	Attitudes indulgentes, croyance en la coopération, langage inoffensif, réputation d'indulgence.
Conscienciosité (*Conscientiousness)*	Aspiration à la réussite (sens aigu des objectifs et niveaux d'aspirations élevés).	Compétences en matière de leadership, plans à long terme, réseau de soutien organisé, expertise technique.

Tableau 1 : Les cinq dimensions de la théorie des personnalités

Pour définir le profil d'une personne, il existe plusieurs questionnaires qui ne peuvent pas être diffusés car ils sont issus d'un ouvrage protégé par des droits d'auteurs et qui s'obtient sous certaines conditions (par exemple avoir un titre de psychologue pour l'édition française).

Ainsi, il existe plusieurs études recherchant quelle dimension de la personnalité est plus susceptible d'être victime d'hameçonnage. Parmi les résultats de ces études, on retrouve une corrélation significative entre les femmes ayant le « Névrotisme » et une plus forte probabilité de cliquer sur un lien d'hameçonnage dans un courriel (Halevi et al., 2013). Toutefois ces résultats sont à prendre avec du recul car l'échantillon est de 100 étudiants en psychologie dont seulement 17 femmes, et l'étude a été réalisée uniquement sur un courriel promettant un gain financier.

Enfin, le modèle descriptif de la personnalité en cinq traits centraux permet de faire un lien entre le genre et la personnalité. Les différences sont assez faibles mais les femmes sont plus souvent névrotiques ou aimables que les hommes (Costa et al., 2001).

Concernant les études réalisées sur ce sujet, on en retrouve avec des paramètres différents :

- Les utilisateurs sont prévenus ou non s'ils font l'objet d'une étude sur l'hameçonnage, donc qu'ils sont susceptibles de recevoir des faux emails.
- Plusieurs types de phishings sont tentés :
    - Des faux courriels de colis à récupérer demandant des informations personnelles,
    - Des notifications de mouvements sur un compte bancaire nécessitant une connexion à un faux site,
    - Des faux courriels de support demandant des informations personnelles pour régler un problème.
    - Des faux courriels de gains
- Une à plusieurs campagnes de phishings, à des intervalles différents,
- Parfois des enquêtes sont envoyés afin d'obtenir plus de détails sur les cibles du phishing et mesurer les publics les plus susceptibles d'être victime du phishing.

Parmi les critères qui ont été analysés, il manque un point important qui est la satisfaction de l'utilisateur. Les outils utilisés par l'utilisateur peuvent lui permettre de se rendre plus facilement compte d'une tentative d'hameçonnage ou non.

Enfin, concernant les publics visés par ces différentes recherches sur l'hameçonnage, certains éléments sont susceptibles de changer la nature des résultats :

- La qualité de l'hameçonnage
    - Le réalisme de la page de phishing ou du courriel envoyé
- La cible du phishing
    - Différences de connaissances dans l'informatique
    - Différences culturelles
- La méthode de recherche (les utilisateurs étaient-ils prévenus, dans un cas réel ou en jeu de rôle, etc)
- Le fait que certaines études comptent un clic et non le fait que l'utilisateur divulgue des données sur ce site. Certains utilisateurs sont curieux et clique, mais ferment ensuite la page sans saisir de données, bien que ce comportement puisse aussi être dangereux (par du code JavaScript malveillant par exemple).

1.1.3. L’impact de la satisfaction des utilisateurs vis-à-vis des mesures de sécurité sur la surface d’attaque

La satisfaction des utilisateurs est aussi un élément lié à divers facteurs, tels que des facteurs techniques et socio-organisationnels.

Ainsi, la satisfaction de l’utilisateur est un élément clé. Les décisions prises aux niveaux des équipes informatiques et notamment des équipes dédiées à la cybersécurité doivent considérer la satisfaction des utilisateurs comme un des principaux critères menant à la réussite de leurs décisions.

Pour cela, il est nécessaire d’avoir le ressenti des utilisateurs vis-à-vis des mesures de sécurité sur les systèmes d’information. Ainsi, trois questions sont posées (Montesdioca & Maçada, 2015):

- Comment les utilisateurs perçoivent-ils leur propre rôle en matière de sécurité de cette information et les mesures administratives de sécurité de l'information dans et les mesures administratives de sécurité de l'information dans leurs processus de travail ?
- Pourquoi les utilisateurs vivent-ils les mesures sécurité de l'information de la manière dont ils le disent ?
- Y a-t-il des arguments dans les opinions des utilisateurs sur la sécurité de l'information qui impliquent des approches alternatives à la gestion de la sécurité de l'information dans les entreprises étudiées ?

Les résultats de cette étude mettent en évidence que les utilisateurs comprennent les avantages des pratiques de sécurité des systèmes d’information, mais que les contrôles de sécurité sont considérés comme question complexe réduisant la productivité des systèmes d’information. (Montesdioca & Maçada, 2015)

Les conclusions de trois autres études sont similaires :

« Une dimension des pratiques de sécurité de l'information est liée au comportement des utilisateurs lors de l'utilisation des systèmes d'information et, par conséquent, des données de l'entreprise. Ces pratiques impliquent un comportement conscient en matière de sécurité lors de l'utilisation des systèmes d'information » (Rhee et al., 2009)

« L'attention portée par les utilisateurs à la sécurité de l'information est associée à une combinaison de facteurs personnels et organisationnels, tels que la satisfaction à l'égard des services de soutien, la satisfaction à l'égard du salaire, la satisfaction à l'égard des collègues, l'engagement organisationnel, les connaissances techniques et les événements émotionnels » (Stanton et al., 2004)

« Les utilisateurs développent des attitudes à l'égard de la sécurité de l'information par le biais de facteurs organisationnels, technologiques et individuels interdépendants. Ces facteurs influencent le comportement des utilisateurs, affectent les motivations concernant le travail avec les pratiques de sécurité de l'information, créent des conflits

d'intérêts entre la fonctionnalité du système d'information et les pratiques de sécurité de l'information, et influencent l'effet de la documentation et des campagnes de sensibilisation sur le comportement de sécurité » (Albrechtsen, 2007)

Ainsi, la satisfaction des utilisateurs semble être un élément plus qu'important pour le respect des mesures de sécurité, ce qui permettrait d'établir un lien entre le respect de ces mesures et la surface d'attaque humaine. Le succès du système d'information et l'acceptation des technologies, comme nous allons le voir dans la suite de l'état de l'art, sont des éléments existants pour garantir la réussite d'un système d'information – dont on pourra considérer que la sécurité des SI en fait partie.

Ces deux éléments sont nécessaires pour trouver une solution permettant le calcul de la surface d'attaque humaine.

1.2. L'Information Systems Success Model pour comprendre le succès d'un SI

1.2.1. L'utilité de la satisfaction utilisateur

La satisfaction de l'utilisateur est un élément clé pour le succès d'un système d'information. L'utilisateur, selon le contexte de l'entreprise, peut aussi bien être un employé, une personne interne à l'entreprise, qu'un client. Il est plus facile d'illustrer l'importance de cette satisfaction par le biais d'un client. Si une entreprise de e-commerce ne parvient pas à satisfaire l'utilisateur vis-à-vis de son système d'information, avec en premier lieu le site internet qui est l'aspect visible de celui-ci pour l'utilisateur, il est très peu probable que cet utilisateur finisse par acheter un produit et qu'il en devienne client.

Toujours à partir de ce même exemple, un site de commerce en ligne est notamment constitué de la partie frontale dont l'aspect et la facilité d'utilisation sont très importants mais la partie non visible, comme la base de données à un rôle très important. Cette base de données est constituée d'informations dont la qualité joue un rôle primordial car ce sont ces informations qui se retrouveront sur le site à la vue de l'utilisateur. Mais outre l'information, le système doit lui aussi être performant et de qualité, car si l'utilisateur doit attendre 30 secondes pour le chargement de chaque produit il s'en lassera rapidement.

Maintenant, observons le modèle de l'Information System Success Model (ISSM) dans sa première version (Figure 3) (DeLone & McLean, 1992).

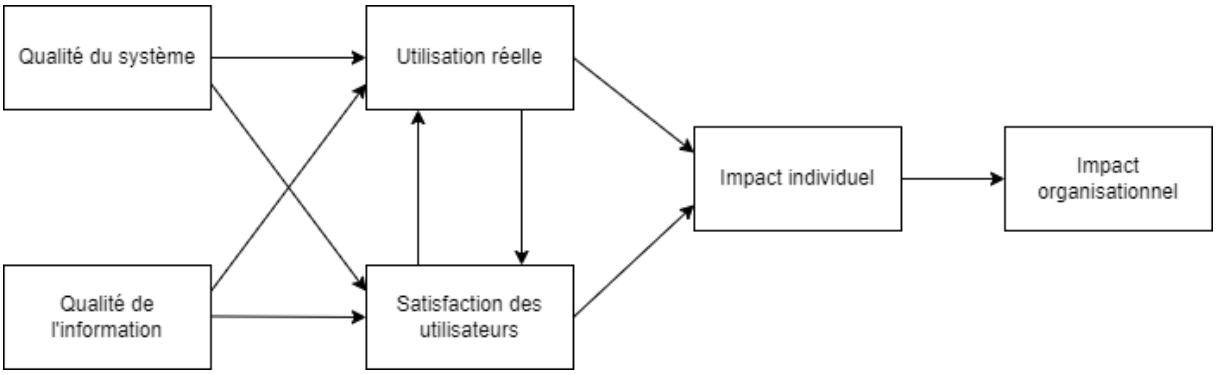

Figure 3 : Traduction du modèle de succès des systèmes d'information (DeLone & McLean, 1992)

Dans ce modèle on retrouve les éléments volontairement avancés dans l'exemple, comme la qualité du système, la qualité de l'information, ces deux éléments impliquent l'utilisation et la satisfaction de l'utilisateur, qui eux-mêmes auront un impact sur l'individu qui se répliquera dans l'organisation.

Tout l'intérêt de ce modèle est dans la personnalisation de ce qui est mesuré pour chacun de ces blocs et c'est même par ce biais que le modèle a été construit (Tableau 2).

Qualité du système	Qualité de l'information	Utilisation du système	Satisfaction de l'utilisateur	Impact individuel	Impact organisationnel
Exactitude des données Valeur des données Contenu de la base de données Facilité d'utilisation Facilité d'apprentissage Commodité d'accès Facteurs humains Réalisation des besoins des utilisateurs Utilité des caractéristiques et des fonctions du système Précision du système Flexibilité du système Fiabilité du système	Importance Pertinence Utilité Caractère informatif Facilité d'utilisation Compréhensibilité Lisibilité Clarté Format Apparence Contenu Précision Concision Suffisance	Quantité d'utilisation / durée d'utilisation Nombre de demandes de renseignements Temps de connexion Nombre de fonctions utilisées Nombre d'enregistrement consultés Fréquence d'accès Nature de l'utilisation • Utilisation aux fins prévues • Utilisation appropriée • Type d'informations utilisées • Objectif de l'utilisation	Satisfaction concernant les spécificités Satisfaction globale Mesure à un seul élément Mesure multi-éléments Satisfaction en matière d'information (Différence entre les informations nécessaires et celles reçues) Plaisir d'utilisation Satisfaction du logiciel Satisfaction de la prise de décision	Compréhension de l'information Apprentissage Interprétation précise Sensibilisation à l'information Rappel d'informations Identification du problème Efficacité de la décision • Qualité de la décision • Amélioration de l'analyse des décisions • Justesse de la décision • Le temps de prendre une décision • Confiance dans la décision • Participation à la prise de décision • Amélioration de la productivité individuelle Changement de décision Causes de l'action de la direction	Augmentation de la part de marché Réduction des coûts d'exploitation Réduction du personnel Gains de productivité globale Augmentation des revenus Augmentation des ventes Portefeuille d'applications : • Gamme et champ d'application Nombre d'applications critiques Augmentation des bénéfices

Sophistication du système Intégration des systèmes Efficacité du système Utilisation des ressources Temps de réponse Délai d'exécution	Complétude Fiabilité Devise Respect des délais Unicité Comparabilité Quantitativité Absence de partialité	Nombre de rapports générés Frais d'utilisation du système Régularité de l'utilisation Utilisation par qui ? (Directe ou guidée) Utilisation binaire • Utilisation vs non-utilisation • Utilisation réelle ou reporté Fréquence des demandes de rapports Niveaux d'utilisation • Général ou spécifique • Utilisation récurrente • Institutionnalisation/routinisation de l'utilisation		Exécution des tâches Qualité des plans Pouvoir ou influence individuelle Valorisation personnelle du système d'information Volonté de payer pour obtenir des informations Qualité de la décision Efficacité des décisions Temps nécessaire à la réalisation d'une tâche Nombre d'objectifs générés Productivité Connaissance de l'ordinateur Confiance dans la décision Capacité à identifier les solutions Quantité de données considéré Précision	Retour sur investissement Rapport entre le revenu net et les dépenses d'exploitation Rapport coût/bénéfice Cours de l'action Augmentation du volume de travail Qualité du produit Contribution à la réalisation des objectifs Augmentation du volume de travail Efficacité des services

		Pourcentage d'utilisation par rapport aux possibilités d'utilisation Volonté d'utilisation Motivation pour l'utilisation		Gain de temps Temps de prise de décision	

Tableau 2 : Résumé des mesures de réussite du mangement des systèmes d'information par catégorie

Pour bien comprendre comment s'applique ce modèle, nous allons prendre un exemple concret et d'actualité qui est celui de la Caisse d'Allocation Familiale (CAF) en réduisant le champ d'application de leur système d'information au seul logiciel de calcul du montant de l'Aide au Logement Social (ALS). Il existe des cas particuliers pour le calcul tel que prévu par la loi, notamment concernant les revenus d'un apprenti qui ne sont pas imposables jusqu'à un certain seuil. Le montant de l'ALS prend uniquement en compte les revenus imposables pour ce calcul sur une période glissante de 12 mois. Ainsi, pour avoir le succès de leur système d'information, ce sont les métriques suivantes qui seraient nécessaires :

Pour la qualité du système, cela comporterait :

- Disponibilité du système
- Temps de réponse
- Flexibilité du système (pour les cas particulier)
- Facilité d'utilisation
- Taux d'erreurs du système

Pour la qualité de l'information, il faudrait prendre en compte :

- L'exactitude des données
- La disponibilité des données
- Ancienneté des données

Concernant l'utilisation du système, il serait évalué par :

- Utilisation d'information numérique vs non numérique
- Fréquence d'utilisation

Pour la satisfaction de l'utilisateur, on mesurerait :

- Satisfaction du logiciel
- Satisfaction globale
- Plainte des utilisateurs
- Différence de satisfaction entre l'attendre et la réalité

L'impact individuel se ressentirais par :

- Temps nécessaire à la réalisation d'une tâche
- Confiance dans la décision

Enfin, l'impact organisationnel serait pris en compte avec :

- Efficacité organisationnelle
- Contribution du système d'information à la réalisation d'objectifs

Concernant la qualité du système, la disponibilité du système, son temps de réponse, sa flexibilité et sa facilité d'utilisation s'explique par la nécessité d'apporter des corrections par les agents de la CAF lors d'erreurs – qui ne sont pas forcément lié au SI. Le taux d'erreurs du système, est par exemple une erreur de calcul des droits d'un allocataire.

Il est important de noter que les auteurs ont écrit : « *This success model clearly needs further development and validation before it could serve as a basis for the selection of appropriate I/S measures. In the meantime, it suggests that careful attention must be given to the development of I/S success instruments.* », ce qui donne en français : « Ce modèle de réussite doit manifestement être développé et validé davantage avant de pouvoir servir de base à la sélection de mesures appropriées du système d'information. Dans l'intervalle, il suggère qu'une attention particulière doit être accordée au développement d'instruments de réussite du système d'information*. »* (DeLone & McLean, 1992)(page 88). C'est ce que nous allons constater par la suite.

1.2.2. L'importance des rétroactions

Avec la nouvelle version du modèle, certaines briques du modèle ont changé notamment pour donner suite à des critiques sur le premier modèle (Seddon, 1997).

Ainsi, l'utilisation réelle est divisée en deux *(Figure 4),* avec l'intention d'utilisation et l'utilisation réelle.

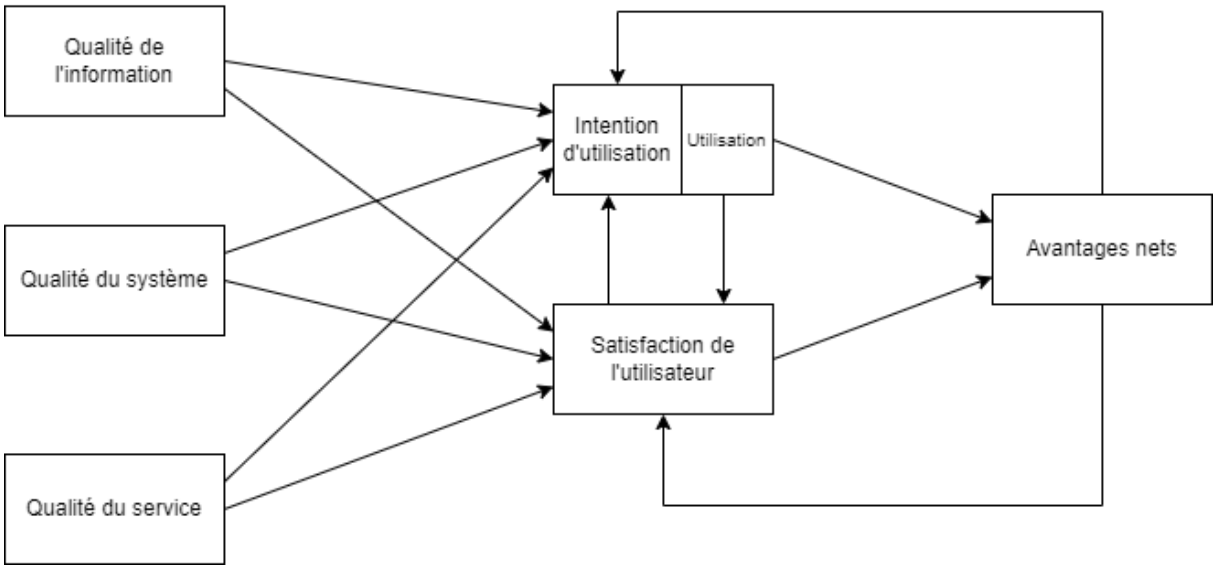

Figure 4 : Traduction de l'ISSM mis à jour (DeLone & McLean, 2003)

Aussi, l'impact individuel et l'impact organisationnel sont réunis en « avantages du système », qui va créer une boucle Avantages du système -> Intentions d'utilisations -> Utilisation réelle -> Avantages du système et une autre boucle Avantages du système -> Satisfaction de l'utilisateur -> Avantages du système. La fusion des deux impacts a pour objectif de rendre le modèle utilisable dans plus de circonstances car d'autres études proposées d'ajouter « impact sociétal », « impact consommation », etc. (DeLone & McLean, 2003)(page 19). Ainsi le terme « Avantages du système » englobe les différents impacts possibles.

Puis la variable qualité du service fait son apparition, essentiellement basée sur les critères du SERVQUAL (Pitt et al., 1995), qui utilise cinq aspects qui sont :

- La tangibilité : les installations physiques, les équipements et l'apparence du personnel.
- La fiabilité : la capacité d'exécuter le service promis de manière fiable et précise.
- La réactivité : la volonté d'aider les utilisateurs et rapidement
- L'assurance : la connaissance et la courtoisie des équipes informatiques et leur capacité à inspirer la confiance et l'assurance envers les outils.
- L'empathie : l'attention donnée à chaque utilisateur est individualisée, au plus proche des besoins de celui-ci.

1.2.3. Revue d'articles basée sur l'ISSM : la quête des variables indépendantes

En 1992, lors du premier article sur l'ISSM, les auteurs titraient cet article comme la quête des variables dépendantes « *Information Systems Success: The Quest for the Dependent Variable* » (DeLone & McLean, 1992). Puis, en 2013, 10 après la mise à jour du modèle de 2003, les auteurs titrent leur article comme la quête des variables indépendantes « *Information Systems Success: The Quest for the Independent Variables* » (Petter et al., 2013).

Tout comme l'article initial, il s'agit ici d'une revue de la littérature concernant les variables indépendantes qui affectent le succès d'un Système d'Information. L'objectif derrière cette troisième étude est de s'interroger sur les éléments externes (indépendants) au système d'information lui-même et qui affecte le succès de celui-ci. On peut citer par exemple, la gestion du support qui consiste à allouer du temps et des ressources afin de soutenir l'utilisation du SI. Les auteurs trouvent ainsi 43 variables dont les 13 plus significatives sont mises en avant (Figure 5).

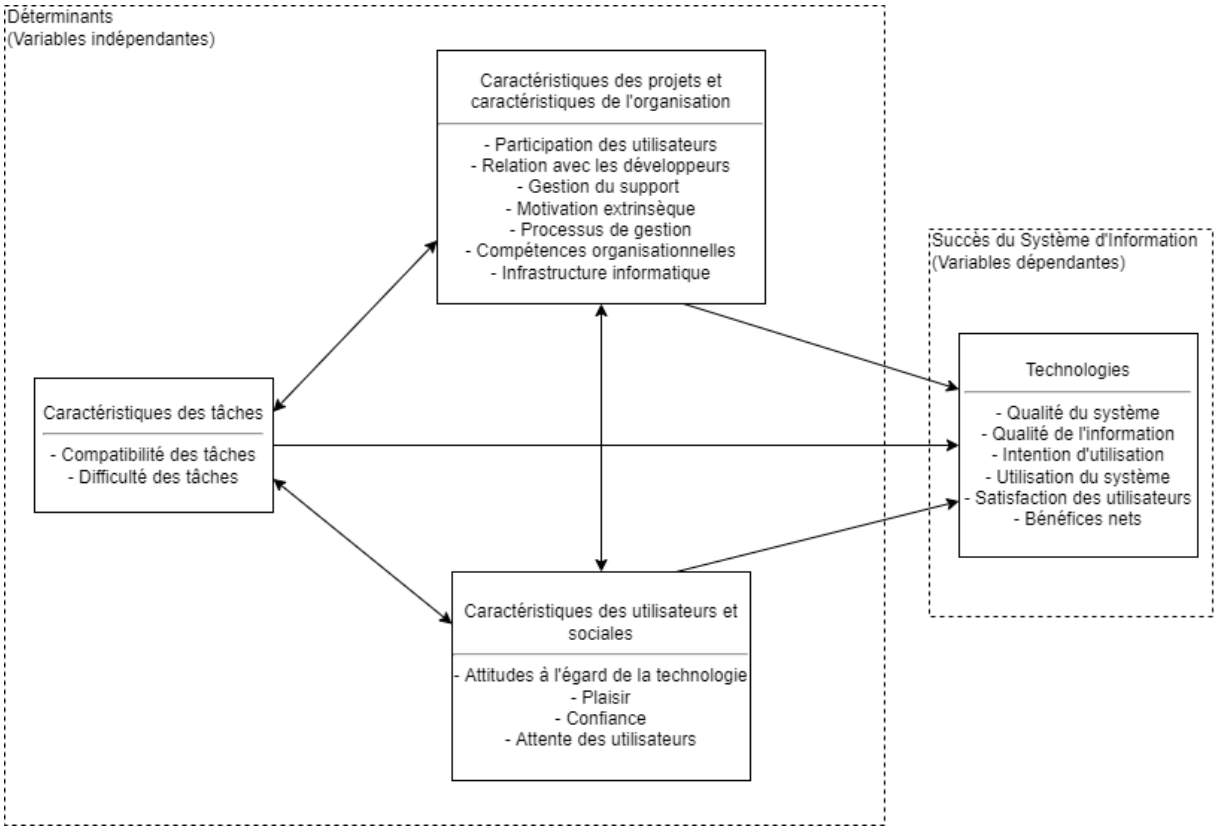

Figure 5 : Variables dépendantes et indépendantes influençant le succès des systèmes d'information (Petter et al., 2013)

On retrouve ainsi la partie des variables indépendantes (zone en pointillé de gauche) et les variables dépendantes (zone en pointillé de droite). Les variables indépendantes interagissent entre elles et vont aussi impacter le système d'information, qui est illustré par les variables dépendantes.

1.2.4. Encore plus de rétroaction : la complexité du succès d'un SI

Enfin, en 2016, une dernière mise à jour est effectuée pour prendre en considération ce qui est appelé « maintenance », c'est-à-dire que l'utilisation du système et la satisfaction des utilisateurs permettent de faire remonter des informations permettant d'améliorer la qualité du système, la qualité de l'information et la qualité du service.

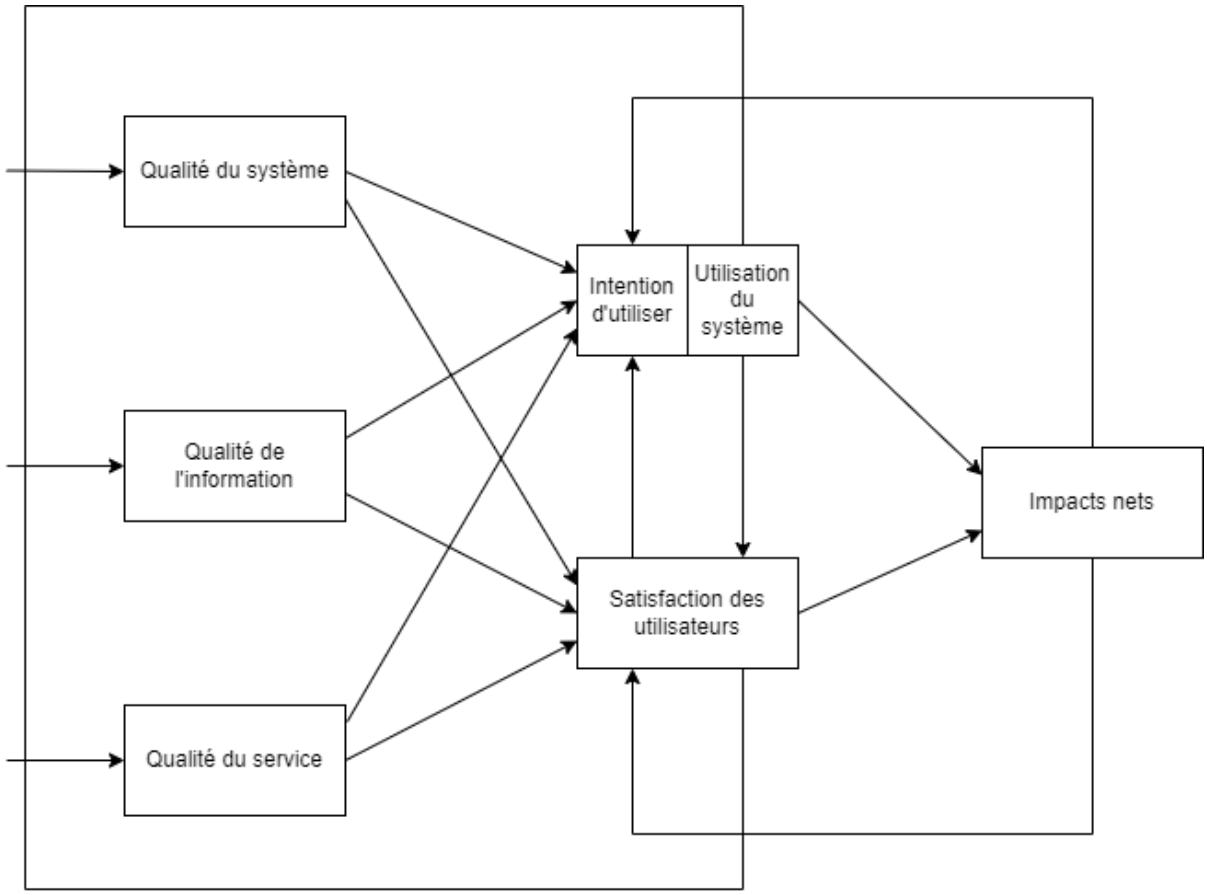

Figure 6: Traduction du Modèle de Delone et McLean mis à jour de 2003 et modifié (DeLone & McLean, 2016)

Il est important de rappeler que derrière ces six dimensions (illustré par un rectangle), ce sont des métriques qui doivent être déterminées par la nature des utilisateurs, des parties prenantes, du niveau d'analyse et du/des but(s) du système d'information.

1.3. L'Intention d'utilisation pour des mesures de sécurité respectées

En lien avec l'impact de la satisfaction des utilisateurs sur le respect des mesures de sécurité, les études concernant l'intention d'utilisation des nouvelles technologies sont

indispensables afin de trouver une solution permettant la réduction de la surface d'attaque et de la calculer à partir des solutions mises en place en partant du postulat qu'elle sera respectée.

Ainsi, il existe plusieurs modèles existants sur l'acceptation des nouvelles technologies, mais nous commencerons ici par le *Theory of Planned Behavior (TPB)* comme le recommande une critique du modèle *Post Acceptance Model* (PAM) qui est le modèle le plus populaire. (Benbasat & Barki, 2007)

1.3.1. La psychologie sociale, domaine clé du facteur humain

L'intention d'utilisation est un aspect appartenant au domaine de la psychologie sociale. Celle-ci s'appuie sur des théories comportementales, comme notamment la théorie de l'action raisonnée (*Figure 7*) (Fishbein & Ajzen, 1975), elle-même améliorée par la théorie du comportement planifié, traduction de *Theory of Planned Behavior (TPB)* (*Figure 8*), (Ajzen, 1991).

Une autre théorie utilisée pour l'intention d'utilisation dans le cadre des nouvelles technologies, est la théorie de la diffusion de l'innovation et son concept d'assimilation des technologies (Rogers et al., 2014).

La théorie de l'action raisonnée (*Figure 7*), prend en compte les croyances comportementales et normatives comme composante de l'intention comportementale, qui mène au comportement effectif.

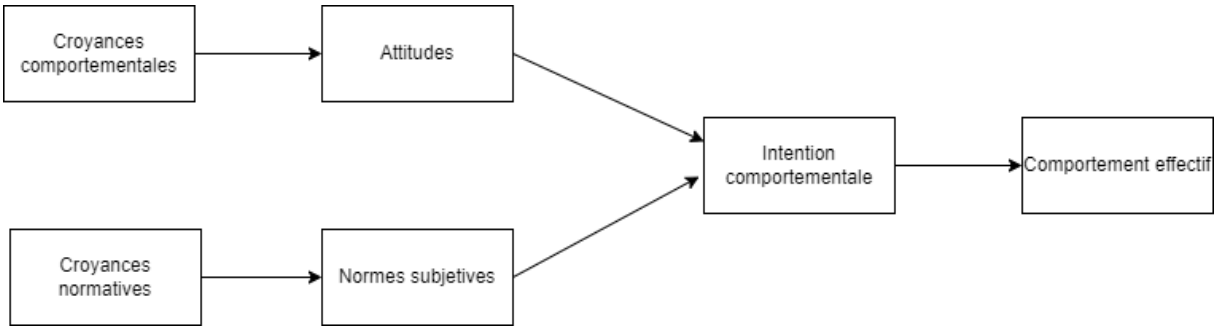

Figure 7 : Traduction de la Théorie de l'Action Raisonnée (Davis et al., 1989)

C'est à partir de cette théorie que celle du comportement planifié a pris racine, notamment avec l'ajout du contrôle comportemental perçu et le changement des interactions entre chaque élément (*Figure 8*).

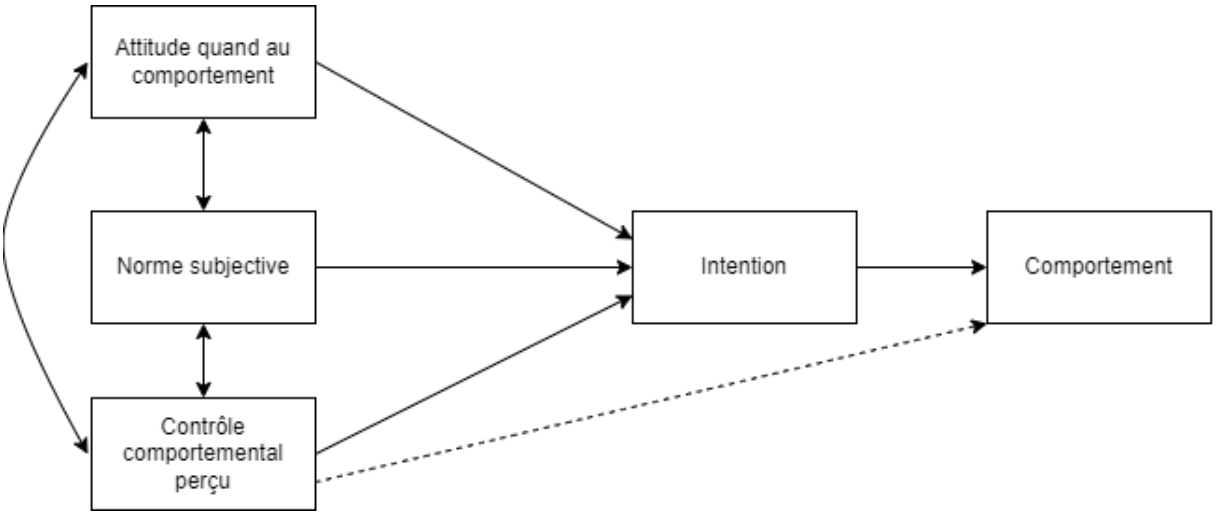

Figure 8 : Traduction de la Théorie du Comportement Planifié (Ajzen, 1991)(page 182)

Ainsi, l'attitude quand au comportement, la norme subjective et le contrôle comportement perçu permettent de prédire les intentions comportementales.

1.3.2. De TAM à UTAUT : prédire l'utilisation d'un SI

Les théories vues précédemment issues de la psychologie sociale ont été adaptés aux systèmes d'information notamment pour l'acceptation des technologies. C'est par une adaptation du TRA que la première version du modèle d'acceptation de la technologie (*Figure 9*), traduit de *Technology Acceptance Model (TAM)* (Davis, 1985), est né. Cette adaptation a eu lieu par l'émergence de trois questions :

- Quelles sont les principales variables de motivation qui interviennent entre les caractéristiques techniques d'un système et son utilisation effective par des utilisateurs ? (traduit de *What are the major motivational variables that mediate between system characteristics and actual use of computer-based systems by end-users in organizational settings ?)*
- Comment ces variables sont-elles causalement en lien entre elles depuis les caractéristiques techniques d'un système, au comportement des utilisateurs ? (traduit de *How are these variables causally related to one another, to system characteristics, and to user behavior?)*
- Comment mesurer la probabilité qu'un utilisateur utilise une nouvelle technologie avant sa mise en œuvre ? (traduit de *How can user motivation be measured prior to organizational implementation in order to evaluate the relative likelihood of user acceptance for proposed new systems?)*

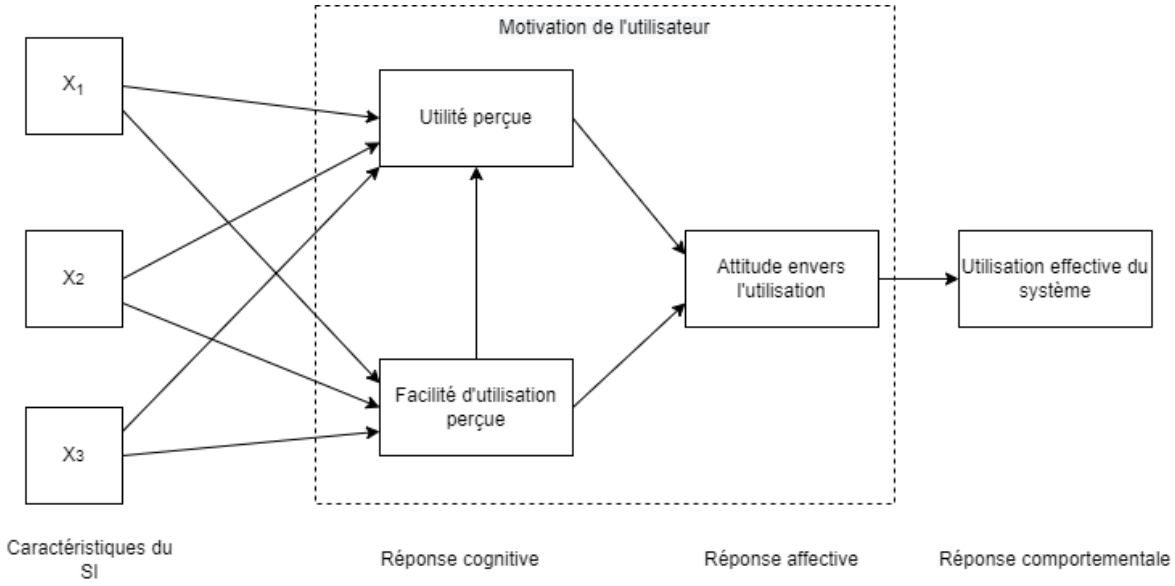

Figure 9 : TAM (Davis, 1985)

L'utilité perçue *perceived usefulness* est la mesure dans laquelle un individu pense que l'utilisation d'un système particulier améliorerait sa performance au travail, là où la facilité d'utilisation perçue *perceived ease of use* (Davis, 1985) est définie comme le degré auquel un individu croit que l'utilisation d'un système particulier serait exempte d'effort physique et mental.

Puis, l'attitude envers l'utilisation *attitude toward using* n'est défini qu'en 2003 dans la proposition du modèle UTAUT comme la réaction affective individuelle concernant l'utilisation d'un système, définition issue de plusieurs modèles et théories : théorie de l'action raisonnée, théorie décomposée du comportement planifié, le modèle de motivation, le modèle d'utilisation des PC et la théorie sociale cognitive.

Enfin l'utilisation effective du système *actual system use*, est défini comme l'utilisation effective d'un système spécifique dans un contexte professionnel. (Davis, 1985)

Par la suite, le modèle a été amélioré par le modèle TAM ci-dessous (*Figure 10*)

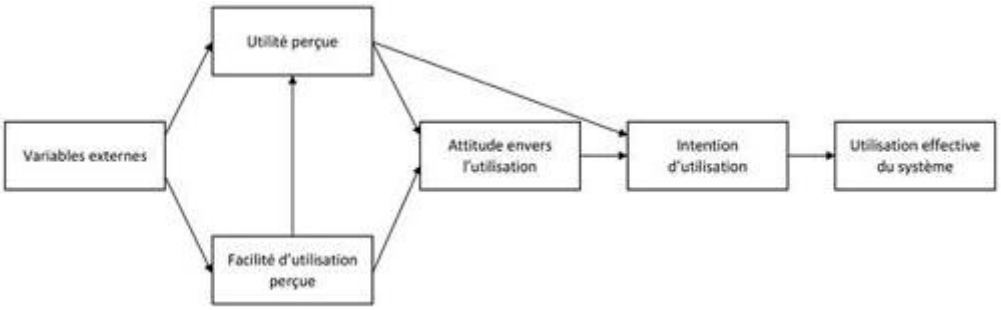

Figure 10 : TAM, seconde mis à jour avant la version finale

On retrouve les mêmes variables avec cependant une variable supplémentaire et des liens différents entre ces variables.

Avec cette nouvelle version (*Figure 11*), on observe un nouvel élément prépondérant qui est l'utilité perçue du système par un individu sur son intention de l'utiliser. Aussi, on est capable de prédire l'utilisation d'un système par un utilisateur à partir de ses intentions Puis, ce travail met en évidence que la perception de la facilité d'utilisation d'un système par l'utilisateur n'est pas un élément déterminant l'utilisation de celui-ci. Enfin, l'attitude envers l'utilisation apparaît comme très peu impactante (ce qui explique le lien entre l'utilité perçue vers l'intention d'utilisation) et se retrouve supprimé dans le modèle final du TAM (à ne pas confondre avec les versions TAM2, UTAUT, etc.).

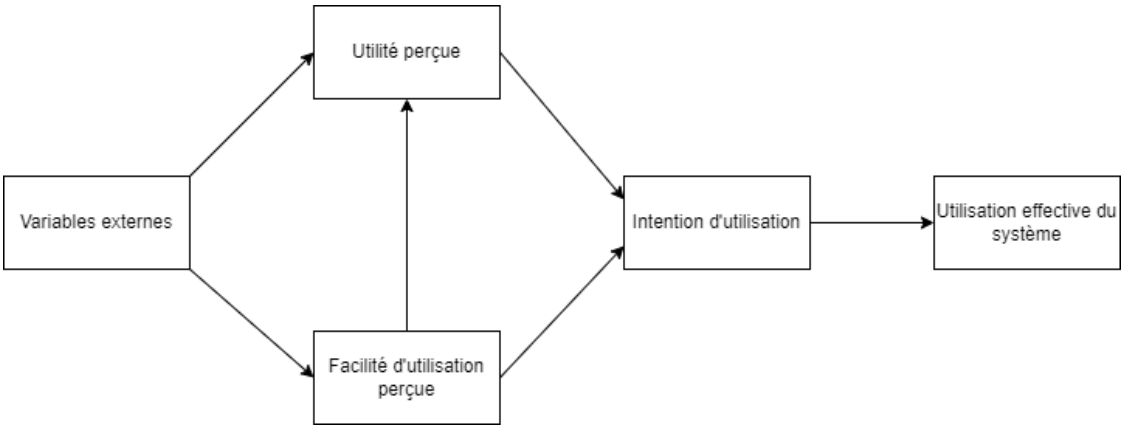

Figure 11 : TAM version finale

Afin de renforcer le modèle TAM, notamment en montrant les variables externes, celui-ci a été mis à jour sans modifier le corps du modèle TAM initial mais en ajoutant des interactions (*Figure 12*).

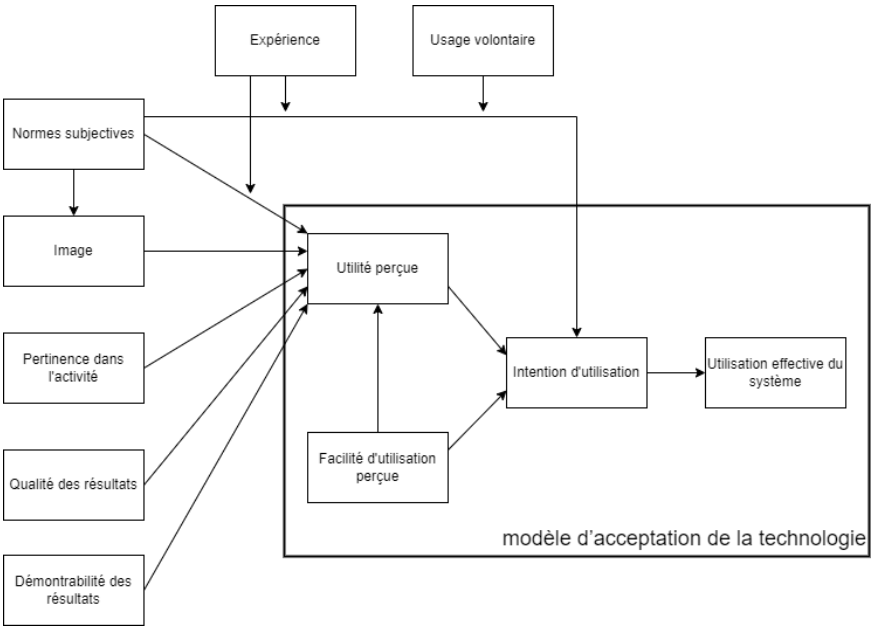

Figure 12 : Traduction du TAM2 (Venkatesh & Davis, 2000)(page 188)

Ainsi, on retrouve les variables suivantes distribuées en plusieurs groupes :

- Les concepts couvrant les processus d'influence sociale
    - Usage volontaire : la mesure dans laquelle les adoptants potentiels perçoivent la décision d'adoption comme non obligatoire (Agarwal & Prasad, 1997; Hartwick & Barki, 1994; Moore & Benbasat, 1991)
    - Normes subjectives : provient de la théorie de l'action raisonnée et est définie comme : la perception de la personne selon laquelle la plupart des personnes qui sont importantes pour elle pensent qu'elle devrait ou ne devrait pas adopter le comportement en question (Fishbein & Ajzen, 1975)(page 302).
    - Image : le degré auquel l'utilisation d'une innovation est perçue comme améliorant le statut d'une personne dans son système social (Moore & Benbasat, 1991)(page 195).
    - Facilité d'utilisation perçue
- Les processus instrumentaux cognitifs
    - Pertinence dans l'activité : la perception d'un individu quant à la mesure dans laquelle le système cible est applicable à son travail. En d'autres termes, la pertinence de l'emploi est une fonction de l'importance, dans l'emploi d'une personne, de l'ensemble des tâches que le système est capable de prendre en charge (Venkatesh & Davis, 2000).
    - Qualité des résultats : l'efficacité d'un système à faire ce qu'il fait (Venkatesh & Davis, 2000).
    - Démontrabilité des résultats : tangibilité des résultats de l'utilisation de l'innovation (Moore & Benbasat, 1991)(page 203).
- Transversale
    - Expérience : impact de l'expérience sur les concepts couvrant les processus d'influence sociale et les processus instrumentaux cognitifs.

Enfin, après ces différents modèles, une étude longitudinale permet d'obtenir un modèle unifié d'acceptation des technologies.

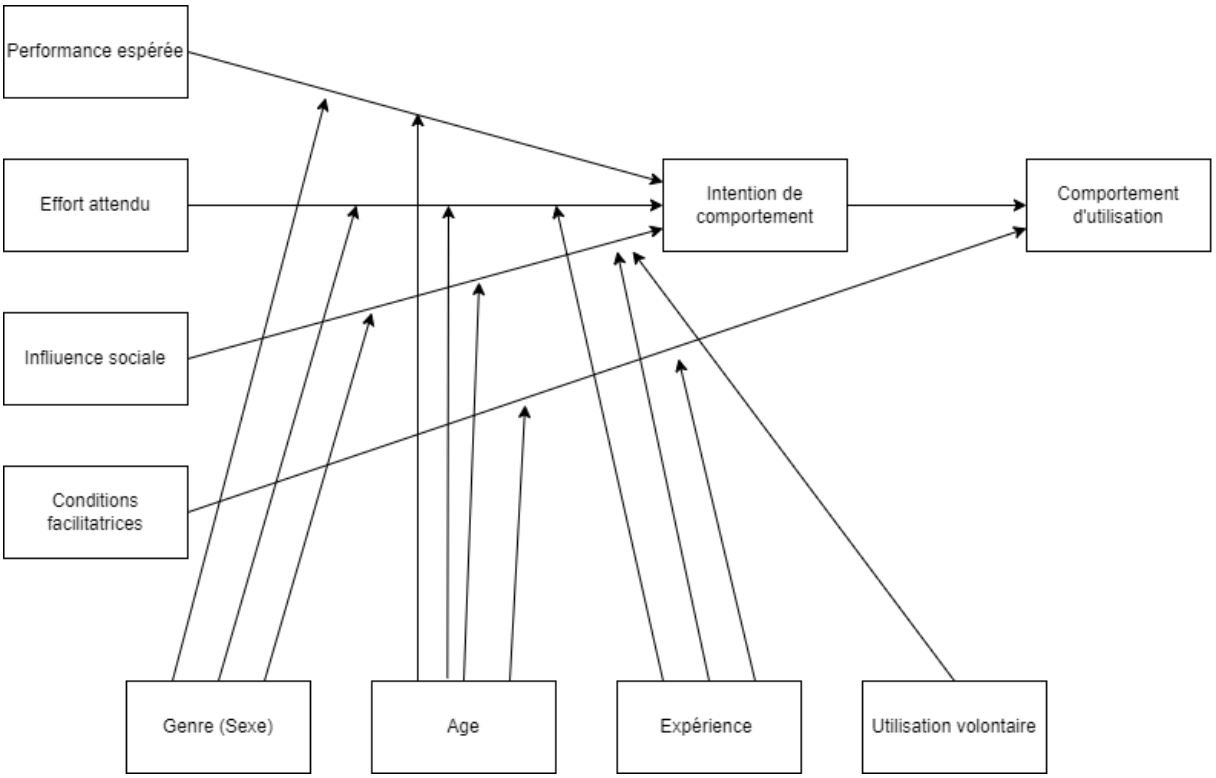

Figure 13 : Traduction de l'UTAUT (Venkatesh et al., 2003) (page 447)

On retrouve ainsi quatre variables significatives qui influent directement sur l'intention de comportement et le comportement d'utilisation, qui sont les suivantes :

- Performance espérée : la mesure dans laquelle un individu croit que l'utilisation du système l'aidera à améliorer ses performances professionnelles.
- Effort attendu : le degré de facilité associé à l'utilisation du système.
- Influence sociale : le degré auquel un individu perçoit que d'autres personnes importantes pensent qu'il devrait utiliser le nouveau système.
- Conditions facilitatrices : la mesure dans laquelle un individu pense qu'il existe une infrastructure organisationnelle et technique pour soutenir l'utilisation du système

Puis, il existe quatre modérateurs qui vont influer ces variables significatives : le sexe, l'âge, l'expérience et l'utilisation volontaire.

L'avantage de cette nouvelle étude est qu'elle met en avant que le modèle UTAUT est capable de mieux prédire l'acceptation et l'usage d'un système par ses usagers.

Depuis les différents modèles observés précédemment, du modèle TAM initial au TAM final, en passant par le TAM2 et l'UTAUT, de nouveaux éléments sont apparus. Bien qu'ils existaient déjà en termes de temporalité lorsqu'ils ont été développés, ils ont fait surfaces en tant que théories pouvant influencer l'acceptation et l'utilisation d'un SI. C'est le cas de la théorie de l'engagement (Joule et al 1998) et du concept de petites actions pouvant influencer le comportement d'une personne d'une manière prévisible (Thaler, 2008).

2. Méthodologie et données

2.1. Objectifs

Dans le cadre de ce mémoire, l'objectif principal est de trouver une solution permettant de définir la surface d'attaque humaine afin de pouvoir estimer l'exposition des systèmes d'information aux risques.

Pour réaliser cet objectif, l'idée est de mettre en évidence qu'il existe un lien entre la satisfaction des utilisateurs vis-à-vis des systèmes d'information et la surface d'attaque humaine.

Ainsi, l'hypothèse est la suivante :

« Il existe une corrélation négative entre la satisfaction des utilisateurs et la surface d'attaque »

Pour valider cette hypothèse, plusieurs questions seront posées afin de connaître pour chaque personne sondée si cette personne respecte ou non les mesures de cybersécurité imposées par leur entreprise. Cela va se faire par des questions séquentielles, partant du propre avis du sondé, à des questions plus subtiles permettant de déterminer si l'avis du sondé correspond à la réalité. Cela grâce à des questions sur le « Shadow IT », où les personnes feront du « Shadow IT » seront considérés comme ne respectant pas les règles de cybersécurité, donc qui augmente la surface d'attaque.

Le « Shadow IT » est l'ensemble des objets et logiciels que les utilisateurs utilisent alors qu'ils ne sont pas mis en place ni recommandés par leur entreprise. Celui-ci peut exister lorsque les utilisateurs recherchent à contourner des mesures trop contraignantes ou pour combler l'absence de logiciel ou outil qui seraient pertinents et utiles pour les usagers des systèmes d'information.

La pandémie du COVID-19 a fait exploser le nombre d'outils non maîtrisés par l'entreprise, comme l'utilisation des ordinateurs personnels ou de solutions comme Zoom pour faire des réunions. Par la suite, les entreprises se sont adaptées pour que cela rentre dans leur périmètre afin notamment d'en avoir un certain contrôle pour éviter la fuite d'information ou d'être victime de piratage.

2.2. Méthodologie suivie

2.2.1. Population choisie

L'objectif de ce questionnaire est de connaître les pratiques existantes mises en place par les Responsables de la Sécurité des Systèmes d'Information (RSSI) et les Directeurs des Systèmes d'Information (DSI) sur la connaissance des utilisateurs et les risques liés. Il s'agit aussi de leur soumettre des propositions afin de connaître leurs croyances mais

aussi de valider des propositions permettant d'obtenir des mesures sur la surface d'attaque humaine.

Outre l'avis des spécialistes des systèmes d'information, il s'agit de connaître le ressenti des utilisateurs sur le système d'information qu'ils utilisent au quotidien au travail puis plus spécifiquement sur les pratiques de sécurité : comment sont-elles perçues, quelles pratiques les utilisateurs appliquent d'eux-mêmes, etc.

Il faudrait idéalement avoir un retour d'utilisateurs issus de métiers différents, dans plusieurs entreprises à des postes similaires. Cependant, les délais pour réaliser le mémoire sont trop courts pour obtenir des autorisations à poser des questions dans plusieurs entreprises et à plusieurs salariés surtout sur un sujet sensible qui est celui de la sécurité et qui peut être vu comme une tentative d'obtenir des informations pour réaliser une attaque. En plus des métiers différents, le positionnement dans la hiérarchie est important pour obtenir l'avis de personnes « VIP » qui n'ont pas les mêmes contraintes qu'un employé « lambda ». Plus ces critères sont respectés, plus l'étude sera de bonne qualité car représentative de la population en entreprise.

2.2.2. Questions posées

Afin de recueillir l'avis d'usagers de systèmes d'information, le questionnaire contient une partie permettant d'avoir une idée sur le public ayant répondu aux questions. Ces questions, à part le genre, sont optionnelles afin de ne pas imposer la récolte de données à caractère personnelles sans que ce soient les utilisateurs eux-mêmes qui décident de les diffuser.

- Votre genre
- Votre prénom
- Votre nom
- Votre adresse e-mail

Puis les deux questions concernant le poste de la personne et son entreprise sont aussi optionnelles. En effet, au vu du sujet, afin d'obtenir le maximum de réponses sans que les personnes aient la crainte que leurs réponses mènent à des représailles ou à un risque de sécurité pour leur entreprise.

- Quelle catégorie de métier occupez-vous ?
- Quelle est votre entreprise ?

Après cette série de question à titre informatif, les questions qui nous intéressent sont les suivantes :

1. Votre entreprise vous impose-t-elle des mesures de sécurité informatique ?

Cette question permet d'avoir une information avec deux interprétations possibles en cas de réponse négative : soit l'entreprise n'a réellement pas de mesures de sécurité

informatique, ce qui est possible dans des TPE et des PME, soit l'utilisateur n'a pas connaissance de ces mesures de sécurité informatique.

2. Comprenez-vous la finalité de toutes ces mesures ?

Cette question permet d'avoir le point de vue des utilisateurs concernant les mesures de sécurité, si un utilisateur ne comprend pas la finalité de certaines mesures, on peut estimer qu'il sera moins susceptible de les respecter.

3. Respectez-vous les mesures de sécurité informatique ? Si non, lesquelles et pourquoi ?

L'intérêt est de voir la proportion de personnes qui ne respectent pas totalement les mesures de sécurité et quelles en sont les raisons.

4. Quel est votre ressenti face aux mesures de sécurité ? Avantages, inconvénients, etc.

Le ressenti des utilisateurs est particulièrement intéressant car il constitue un élément de leur satisfaction et du risque que ces utilisateurs passent outre ces mesures.

5. Utilisez-vous des outils qui ne sont pas directement fournis par votre entreprise ? Lesquels ? (ordinateur, téléphone, etc.)

En plus du respect des mesures de sécurité, il est important de savoir si les utilisateurs utilisent d'autres outils pour des usages professionnels et qui ne sont pas sous le contrôle de leur entreprise. Cela a pu être le cas lorsque des confinements lors de la pandémie de COVID-19.

6. Utilisez-vous des applications/logiciels qui ne sont pas mis à disposition par votre entreprise ? Lesquels ? (Par exemple whatsapp pour des communications professionnelles alors que votre entreprise met teams à disposition)

Il est important d'identifier à quelle fréquence des logiciels sont utilisés alors qu'ils ne sont pas sous le contrôle de l'entreprise et qui ne peuvent donc pas faire l'objet de règles particulières. L'ensemble des outils utilisés en dehors du SI de l'entreprise peut être nommé le « Shadow SI », c'est-à-dire le système information de l'ombre.

7. Sur 10, quelle est votre satisfaction globale concernant le système d'information de votre entreprise, y compris les mesures de sécurité imposées ? Pourquoi ?

Enfin, une question pour connaître la satisfaction globale des utilisateurs vis-à-vis du système d'information, afin d'essayer d'établir un rapport entre le respect des mesures et la satisfaction des utilisateurs.

Derrière ces questions, l'objectif est de pouvoir établir des liens entre la satisfaction des utilisateurs et le respect de mesures de cybersécurité.

Concernant les mesures de sécurité, ce qui est recherché par des questions qui se développent petit à petit, permettant de savoir si le répondant considère qu'il respecte ou non les règles de sécurité et peut développer la réponse pour avoir des nuances. Puis les questions concernant l'utilisation des outils personnels ou l'utilisation des logiciels qui ne sont pas mis à disposition par l'entreprise vont permettre de détecter les personnes qui pensent respecter les mesures de sécurité mais qui pourtant utilisent des outils représentant un plus grand danger et qui ne sont de manière très générale pas autorisés par les politiques de sécurité des systèmes d'information.

Pour cela, l'évolution sera mesurée par des graphiques comparant le pourcentage de personnes respectant les règles contre le pourcentage des personnes ne les respectant pas.

Enfin, l'outil Iramuteq sera utilisé pour réaliser une analyse de similitude (ADS). « L'ADS est une technique, reposant sur la théorie des graphes, classiquement utilisée pour décrire des représentations sociales, sur la base de questionnaires d'enquête (Flament, 1962) (Flament, 1981) (Vergès & Bouriche, 2001) » (Marchand & Ratinaud, 2011). Ainsi, cela permettra de comprendre la perception de certains mots clés par les utilisateurs et à quoi ils les associent.

2.3. Données des entretiens

2.3.1. Nature des participants

Le nombre de personnes ayant répondu aux questions est de 24 personnes, cependant une personne ayant répondu seulement « m » à la question « Respectez-vous les mesures de sécurité informatique ? Si non, lesquelles et pourquoi ? », cet avis ne sera pas pris en compte. Le nombre de répondant confirmé est donc de 23 personnes.

Le premier résultat obtenu est à titre indicatif, parmi les répondants, 29% sont des hommes et 71% sont des femmes. L'équilibre n'est pas obtenu mais en considérant l'état de l'art qui tend à montrer que les femmes sont plus susceptibles au phishing par exemple, on peut se dire qu'il s'agit d'une bonne chose que le public considéré comme plus à risque soit majoritaire à répondre pour ce mémoire.

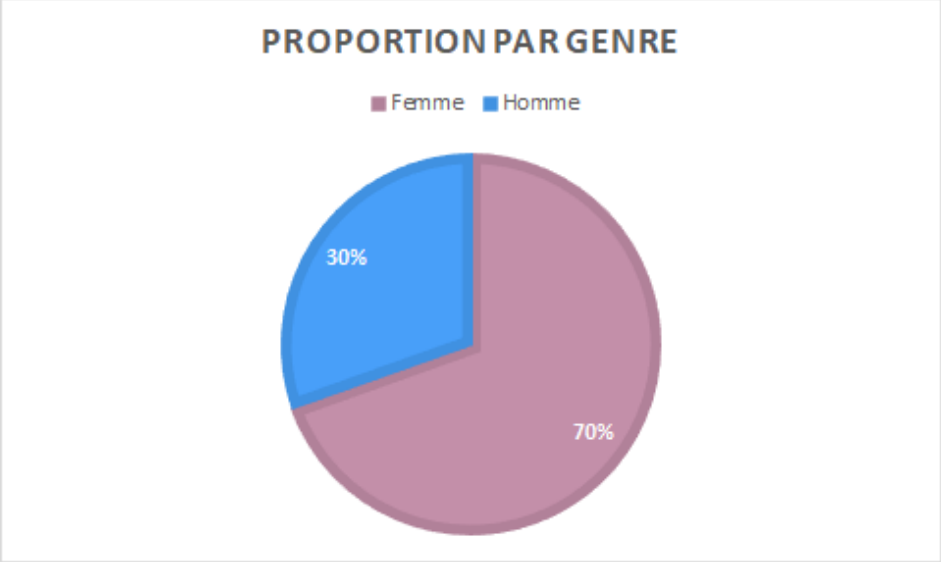

Figure 14 : Proposition des répondants par genre

La répartition du secteur entre service public et entreprise privée est déséquilibrée, avec une surreprésentation puisque 67% (quasiment trois personnes sur cinq), des interrogés travaillent dans le service public, alors que d'après l'Insee, seulement un salarié sur cinq travaille dans la fonction publique. (*Insee,* 2022) Une seule personne n'a pas répondu et il est fort probable, au vu des personnes sollicitées, que ce soit une personne travaillant dans une entreprise privée.

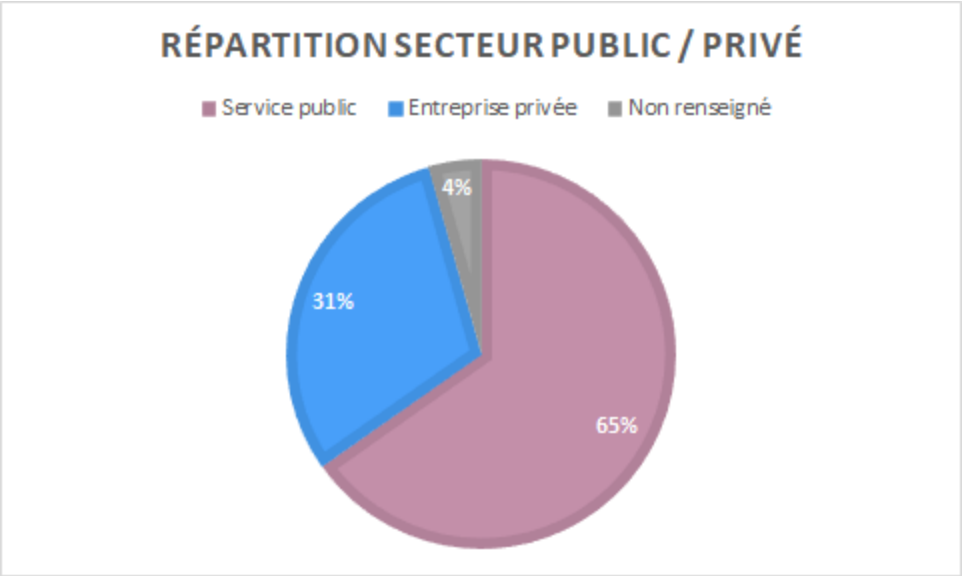

Figure 15 : Répartition public/privé

Toutefois, ce déséquilibre ne devrait pas poser de problème puisque les métiers représentés ne sont majoritairement pas liés à l'informatique (seulement 3 répondants font de l'informatique), donc ce sont les principaux usagers des systèmes d'information qui sont sollicités.

3. Résultats et discussions

3.1. Analyse des résultats

Après les questions d'ordres générales pour connaître les sondés, la première concerne les mesures imposées par l'entreprise (Figure 16). Une seule personne a répondu que son entreprise n'impose pas de mesure de sécurité. Cette personne travaille dans un hôpital public, il est difficile de ne pas faire un lien, un peu simpliste, entre le nombre d'attaque subit par les hôpitaux publics ces derniers mois et ce qui semble être l'absence de mesure sécurité pour le personnel soignant. Les milieux médicaux sont un cas assez unique et impactés par plusieurs aspects.

Notamment, il y a actuellement un manque crucial de personnels et l'ajout de mesure de sécurité qui risquerait de ralentir la cadence du personnel soignant pourrait dégrader la santé des patients. Ce point est soulevé pour mettre en lumière que le respect des mesures de sécurité ne sont pas uniquement liés au système d'information lui-même.

Cependant, le monde médical nécessite d'autant plus d'être sécurisé pour ces mêmes raisons, puisque l'arrêt des systèmes d'information des hôpitaux ralentissent la prise de connaissance des pathologies des patients, de leurs résultats d'analyses, radio, IRM et ainsi de suite. De plus, les données de santé sont particulièrement sensibles. Le monde médical est un sujet très important et qui met en évidence les difficultés qui apparaissent pour mettre en place des mesures de sécurité, qui nécessite de former le personnel et de ne pas ralentir l'activité, en plus d'un coût économique élevé.

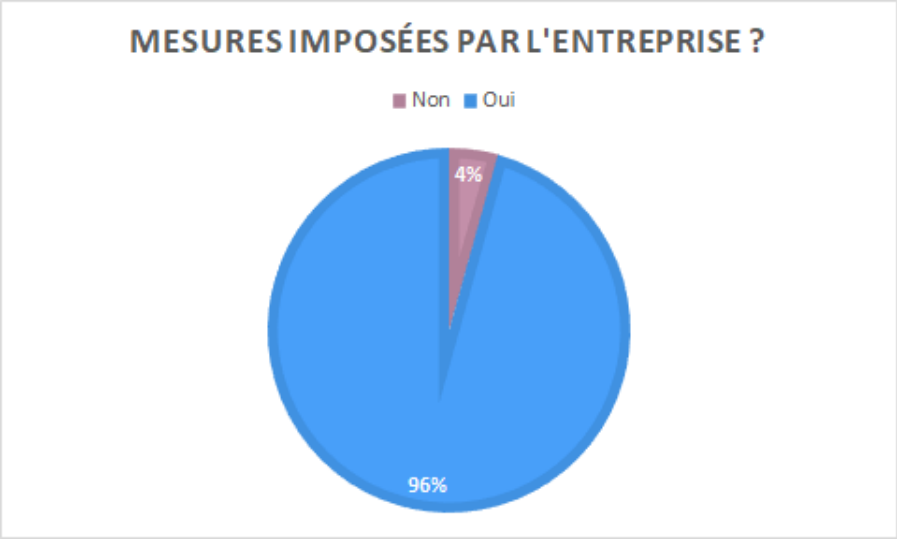

Figure 16: Résultats sur la présence de mesures imposées par l'entreprise ou non

Enfin, on pourrait aussi considérer que cette réponse « non », ne reflète pas spécifiquement les mesures existantes dans l'entreprise mais plutôt la connaissance de ces mesures par les usagers du système d'information.

Dans tous les cas, le reste des résultats s'effectuera sans prendre en compte cette personne interrogée afin de ne pas ajouter un biais, ce qui nous amènent à 22 répondants.

Parmi ces 22 répondants, les mesures imposées sont comprises par 95% des personnes (Figure 17).

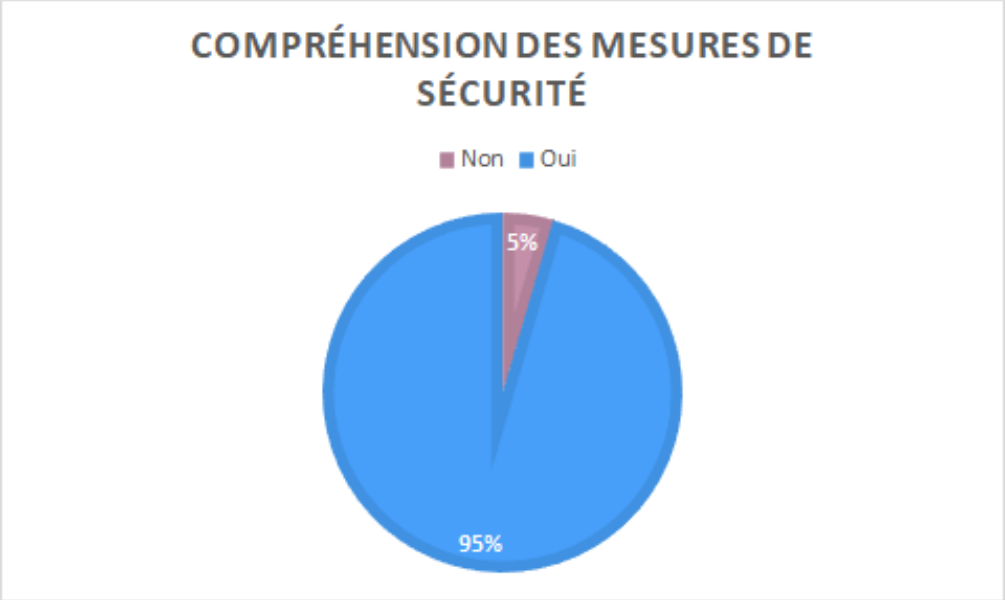

Figure 17 : Compréhension des mesures de sécurité sur les 14 réponses Oui

Elles sont aussi revendiquées comme respectées par 86% des interrogés (Figure 18).

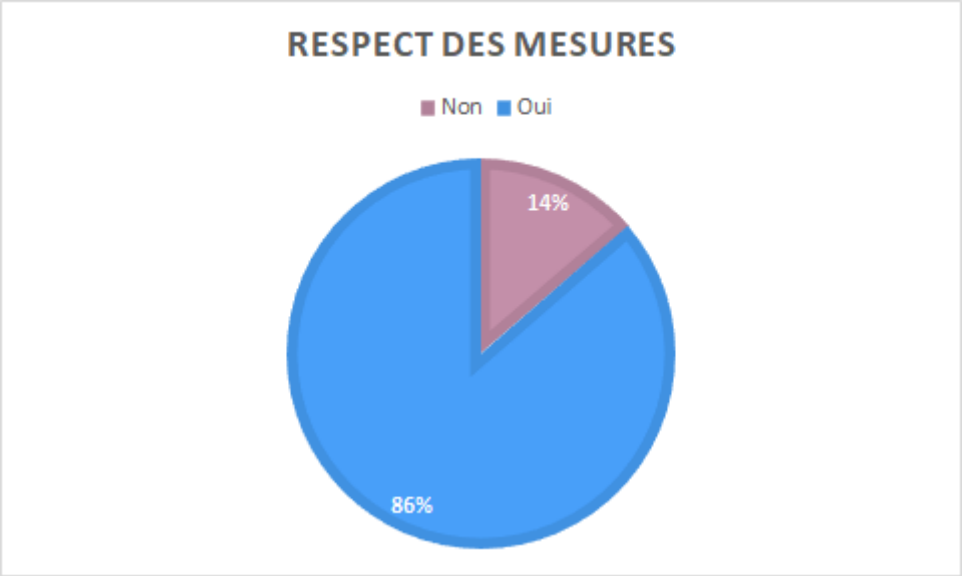

Figure 18 : Respect des mesures en tenant compte du "Oui" ou "Non" des interrogés

Cependant, si on prend en compte les nuances dans les réponses, on tombe à 74% qui respectent réellement les mesures (Figure 19). En effet, il y a certaines nuances telles que : « oui, sauf la tenue d'une liste de mots de passe utilisés au bureau. », « Dans l'ensemble, les mesures de sécurité sont respectées. » ou encore « Oui, le changement de mot de passe mais […] je les écrits sur post-it ».

On remarque dès lors, que les utilisateurs en premier lieu affirment respecter ces mesures tous en admettant que finalement ils font quelques manquements. Mais c'est bien ce « Oui » qui ressort en premier plutôt que d'affirmer que « Non » sur certains points. C'est bien ce ressenti qu'il faut réussir à obtenir pour parvenir à quantifier la surface d'attaque humaine par le manquement à des mesures de sécurité, ne serait-ce pour mieux en comprendre les raisons et améliorer les mesures de sécuritées pour qu'elles soient plus amplement respectées.

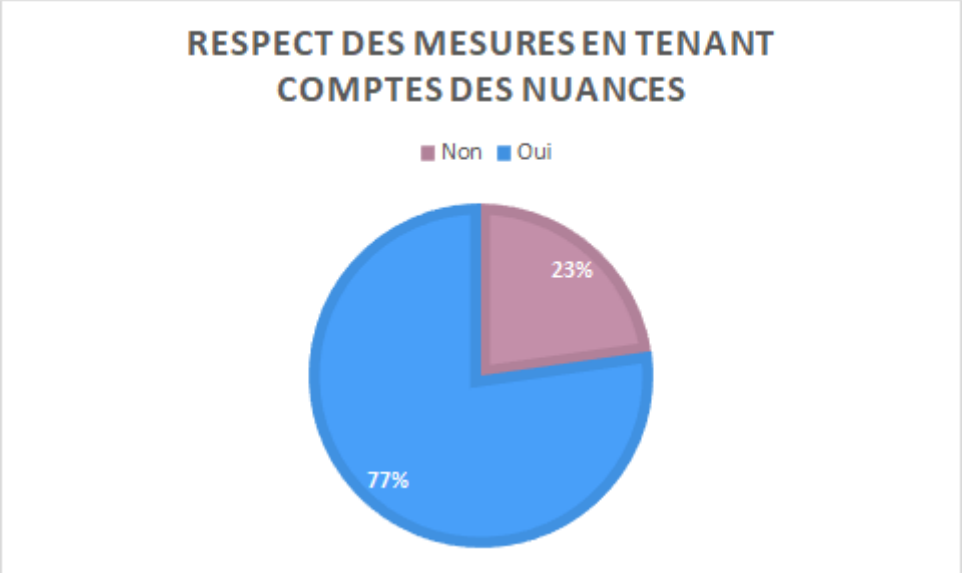

Figure 19 : Respect des mesures de sécurité selon les propos des interrogés

Enfin, pour terminer en ce qui concerne le respect des règles de sécurité, un nouveau graphique a été réalisé en considérant comme une personne ne respectant pas les mesures de sécurité ceux qui ont répondu positivement aux questions concernant l'utilisation d'objets ou de logiciels qui ne sont pas mis à disposition par l'entreprise. En effet, l'utilisation d'un logiciel qui n'est pas pris en compte dans le périmètre de l'entreprise ou d'une machine personnelle entraine un risque supplémentaire puisque cela empêche de mettre des sécurités adéquates pour ces outils. (Figure 20)

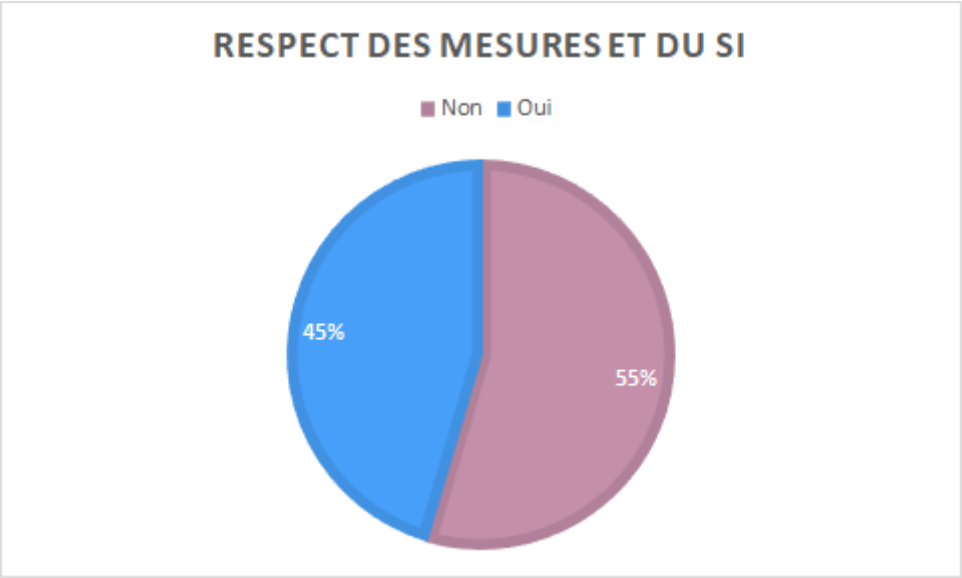

Figure 20 : Respect des mesures en considérant le "Shadow IT" comme un non-respect des règles

Le nombre de question et leur orientation permet d'avoir une forme d'effet entonnoir ce qui tend à obtenir des réponses reflétant au mieux la réalité. Le graphique ci-dessous permet de mieux visualiser cet effet à titre indicatif (Figure 21). L'intérêt de ces questions est que cela met en évidence les biais des utilisateurs, de leur sentiment de respecter les règles alors qu'ils en font des entorses. On retrouve ce même type de comportement chez les usagers de la route, où des personnes se pensent dans les règles et se rendent compte, au fil de questions poser, qu'ils ne respectent finalement pas les règles qu'ils pensaient respecter.

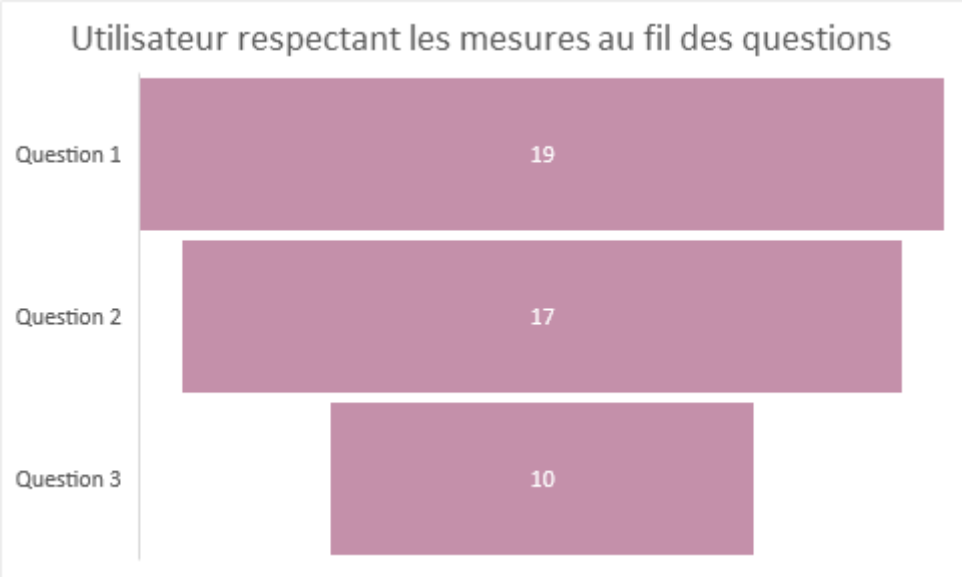

Figure 21 : Effet entonnoir au fil des questions

Outre le respect des mesures, il est intéressant de mettre en perspective la satisfaction des utilisateurs et leur respect ou non des mesures, en prenant ne compte

l'utilisation d'outils non mis à disposition par l'entreprise comme un non-respect des mesures de sécurité. Une personne n'a pas mis de note de satisfaction mais la réponse suivante : « Bof je n'aime pas le fait que j'utilise mon téléphone », il y aura ainsi que 21 réponses pour la comparaison entre la satisfaction des utilisateurs et le respect des mesures de sécurité. On remarque qu'une rupture apparaît dès lors que la satisfaction des utilisateurs est égale ou inférieure à 7 sur 10, mais ne permet pas d'être certain qu'une personne notant sa satisfaction à 7 ou moins ne respectera pas les règles (Figure 22).

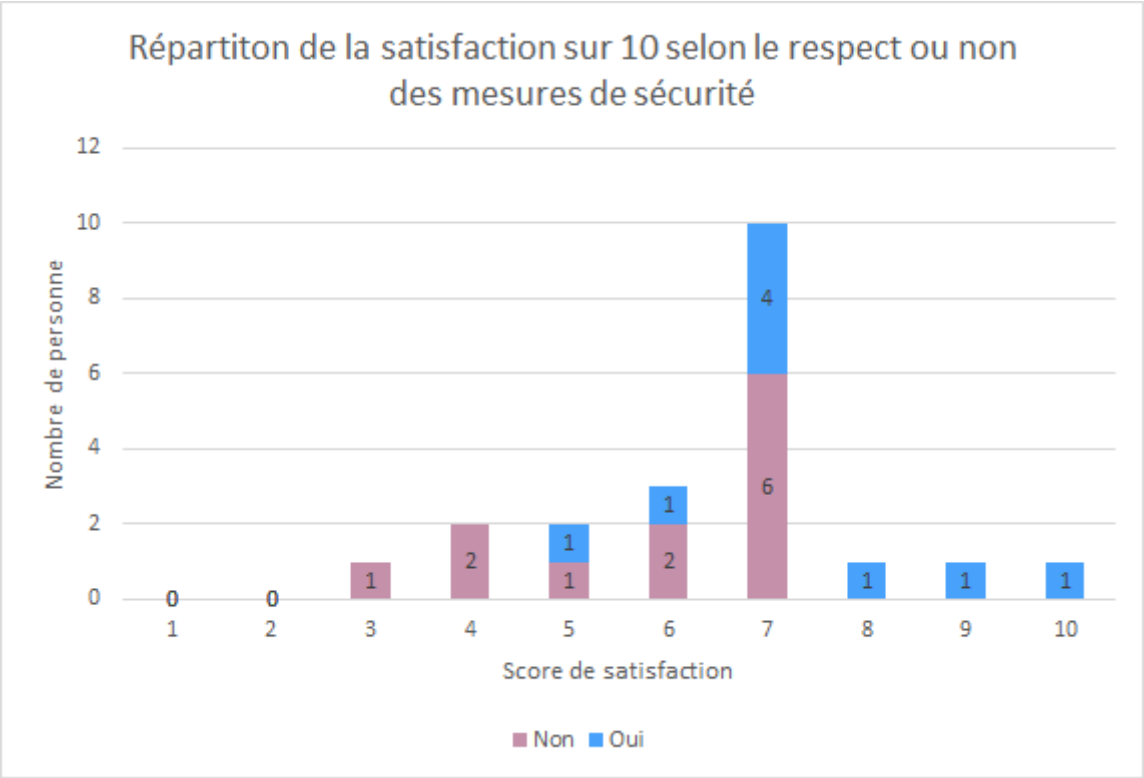

Figure 22 : Satisfaction des utilisateurs selon le respect ou non des règles de sécurité, avec le « Shadow IT » considéré en « Non » respect de ces mesures de sécurité.

Enfin, en ce qui concerne ce qui a été exprimé par les utilisateurs par rapport aux règles de sécurité et à leurs satisfactions, on retrouve les représentations suivantes (Figure 23) :

La sécurité est bien associée à l'informatique, ce qui est vu comme contraignant et imposé par l'entreprise. Cette sécurité informatique renvoie vers cinq communautés dont trois nous intéressent (les autres ne donnant pas d'informations essentielles, mais apparaissent notamment à cause du corpus qui est peu volumineux) :

- Les utilisateurs associent les mots de passe (**multiplicité**) à une **obligation**, qui nécessite d'être modifié régulièrement (**changement**). Ces **mots de passe** sont **utilisés** pour la **sécurité** informatique (lien entre diverses communautés).

- L'informatique est vu comme un **outil**, permettant le **travail,** notamment au sein d'un **ministère** *(cela est dû au nombre élevé de répondant issue de la fonction publique).*

- La sécurité est **nécessaire**, mais **prend** du **temps**.

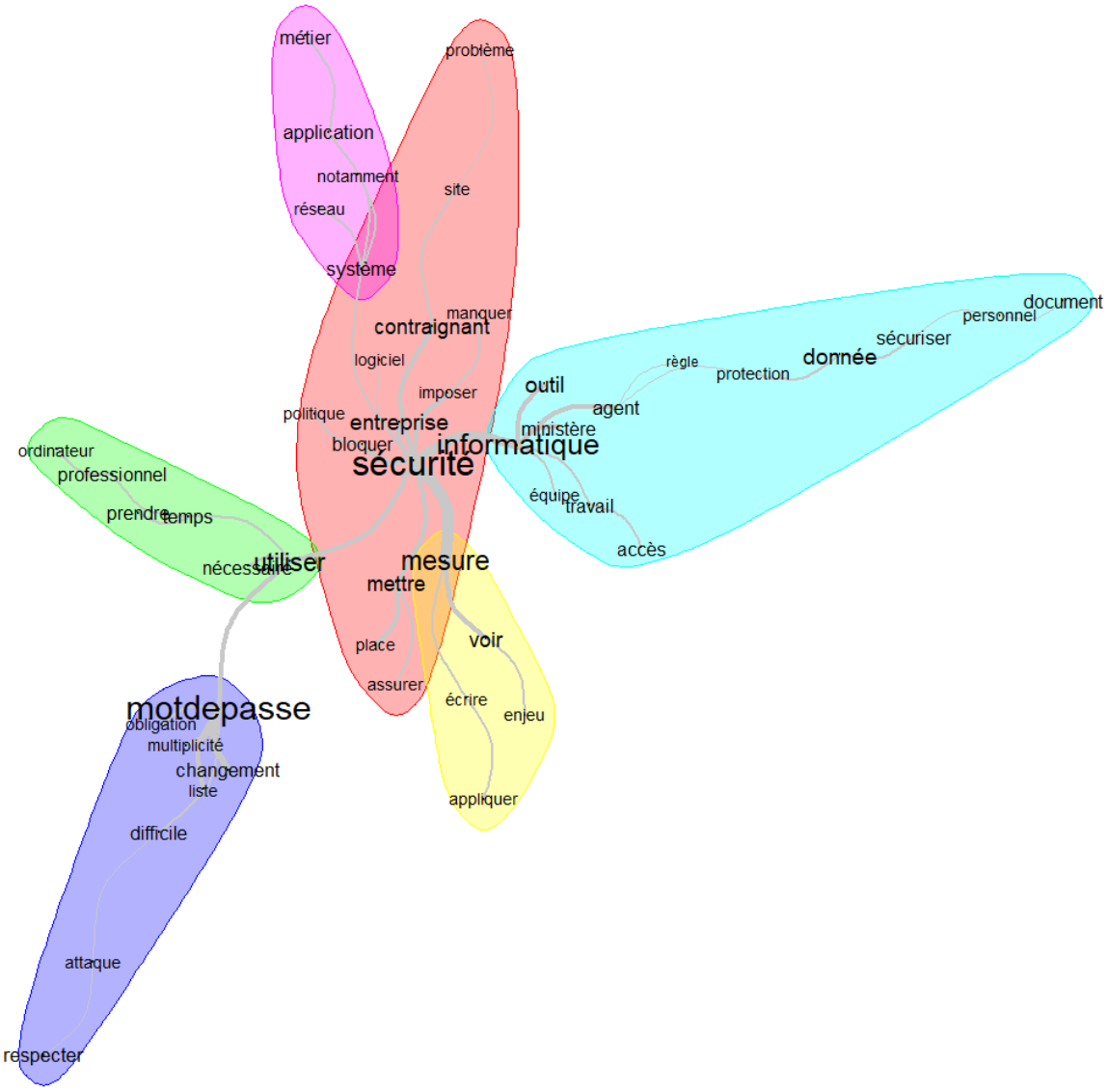

Figure 23 : Analyse des similitudes issue d'Iramuteq

Ainsi, la représentation de la sécurité informatique les utilisateurs montrent qu'ils comprennent l'utilité de ces mesures mais qu'elles sont chronophages et difficiles à appliquer. Un enjeu pour réduire la surface d'attaque serait de trouver des solutions moins difficiles à appliquer, idéalement transparente pour les utilisateurs.

3.1.1. Conclusion sur ces données

Ces données montrent que la question de confiance est un élément important pour la sécurité des systèmes d'information. À la fois les répondants font majoritairement confiance aux mesures de sécurité en vigueur, et à la fois ils semblent avoir particulièrement confiance en eux-mêmes pour le respect de ces règles. Cela entre en contradiction avec les statistiques sur les cyberattaques et met en évidence que la nature et la réalité des risques ne sont pas forcements compris, menant à des comportements dangereux. L'hypothèse « Il existe une corrélation négative entre la satisfaction des utilisateurs et la surface d'attaque » semble plausible au vu des résultats mais l'échantillon est trop faible pour valider cette hypothèse par des tests statistiques.

3.2. Apports et recommandations de ce mémoire

3.2.1. Coefficient par population

Un premier principe permettant de mesurer le risque informatique lié aux utilisateurs est d'effectuer une pondération selon des critères établis par l'entreprise elle-même. Cela en prenant en compte son secteur d'activité et sa connaissance des systèmes d'information permettant de savoir quels métiers sont les plus susceptibles de mettre l'activité de l'entreprise en danger.

Ce coefficient ne serait pas quantitatif mais qualitatif, sur une échelle comme pour la méthode d'analyse de risque EBIOS, avec des informations qui pourraient être issues d'une solution d'IAM (Gestion des identités et des accès) et d'autres plus subjectives.

L'idée est d'avoir une vision complète de l'entreprise (Figure 24), notamment avec un organigramme qui donnerait des indicateurs selon certains critères. À titre d'exemple, pour la partie IAM combiné avec les différents services d'une entreprise, on retrouverait les accès à privilège ou non.

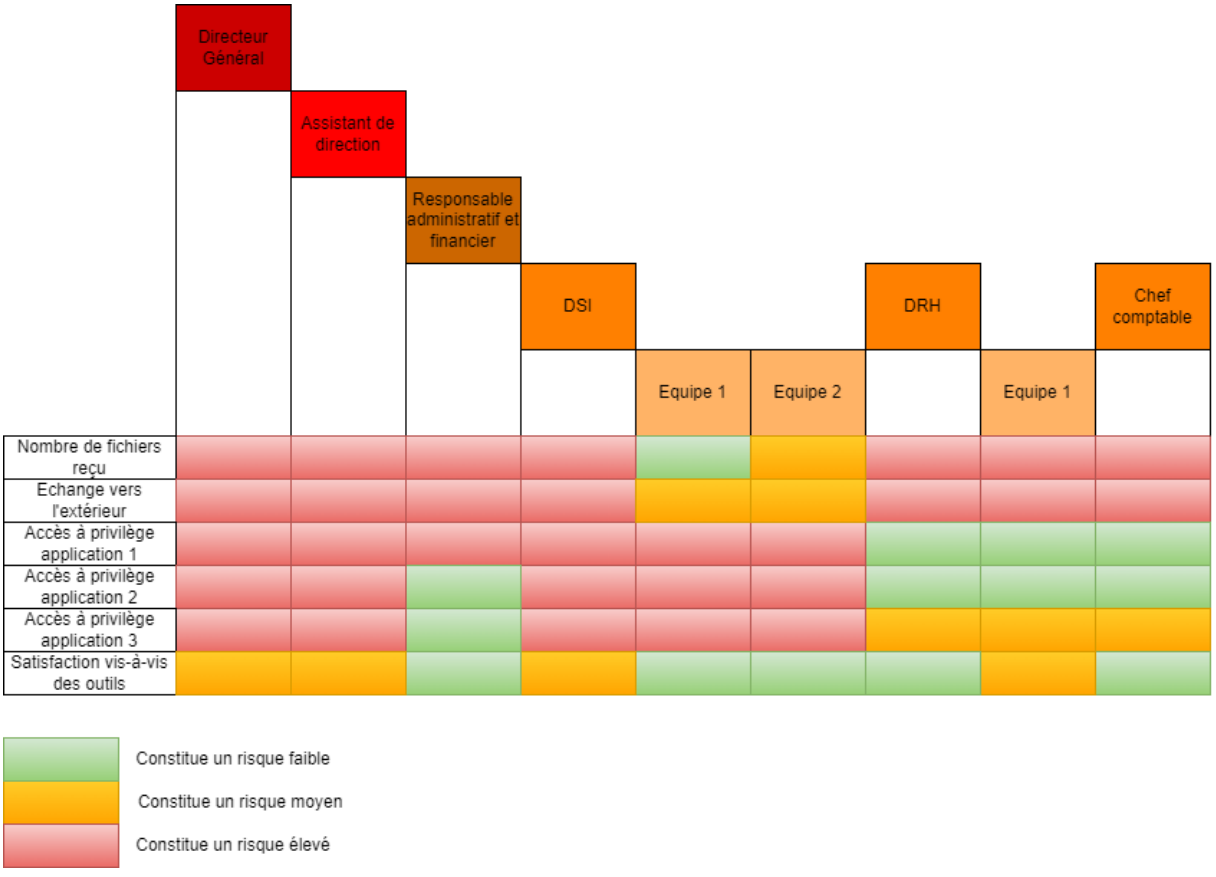

Figure 24 : Organigramme avec risque par département

Puis, on retrouve des informations permettant de savoir s'il s'agit d'un service susceptible de recevoir beaucoup de fichier ou d'être en contact avec beaucoup de personnes extérieures à l'entreprise. Ainsi, le service DRH serait plus à risque pour les fichiers au vu des candidatures qui peuvent très bien contenir un faux CV malveillant.

3.2.2. Security Measure Success model

L'ajout des mesures de sécurité va impacter le succès d'un système d'information par plusieurs biais. Ainsi, on reprend le modèle de succès des systèmes d'information en ajoutant les mesures de sécurité (Figure 25).

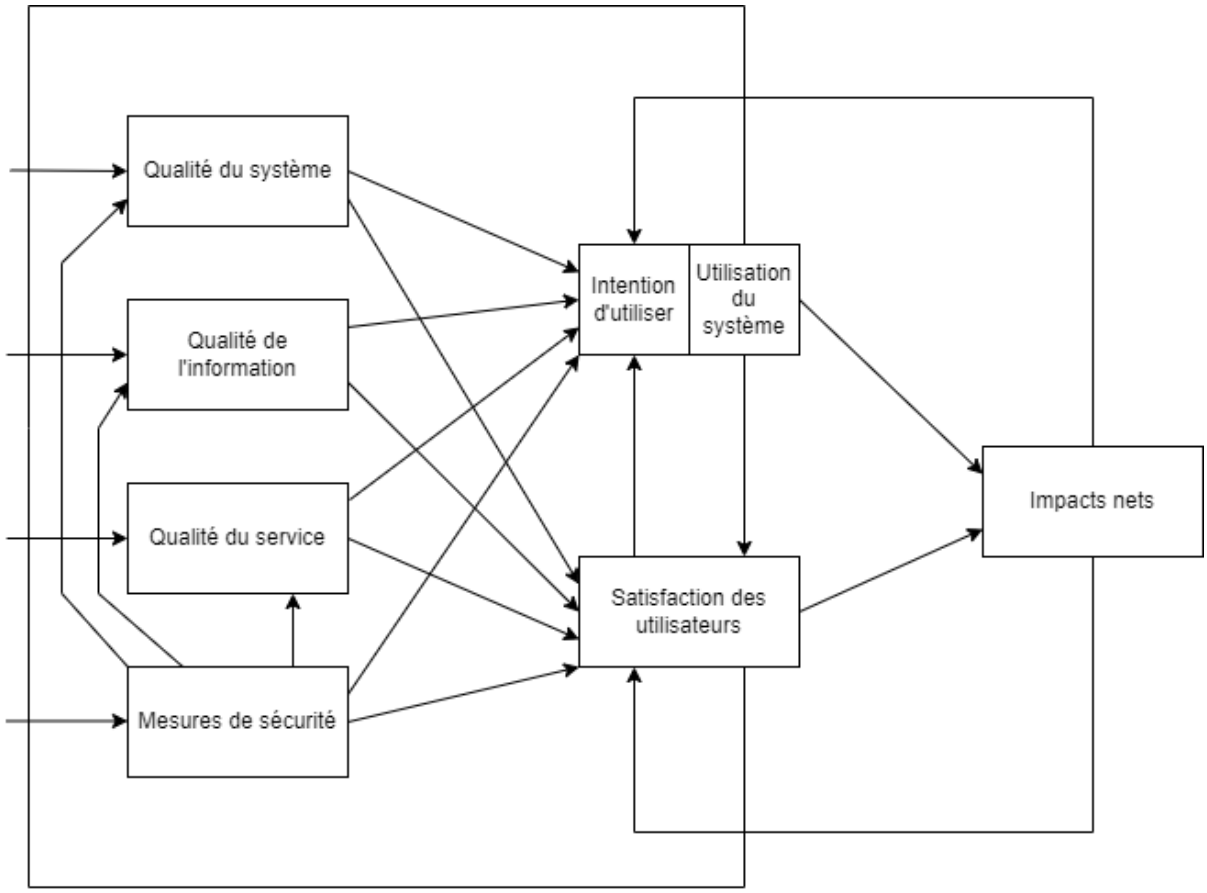

Figure 25 : Proposition du Security Measure Success Model

Premièrement, les mesures de sécurité, par leur respect, vont renforcer la qualité de l'information car en l'absence d'attaque, les informations ne pourront pas être altérées par une action malveillante.

Deuxièmement, la qualité du système peut être dégradée comme améliorée par les mesures de sécurité selon comment elles sont implémentées. Par exemple, une mesure de chiffrement mal positionnée peut générer une forte lenteur.

Troisièmement, le facteur le plus impacté est celui de la qualité de service. Les mesures de sécurité rajoutent un travail aux équipes support utilisateurs avec les problèmes que cela peut causer, comme le blocage d'une application suite à plusieurs tentatives de mot de passe ayant résulté à un échec.

Puis, les mesures de sécurité vont directement changer la perception des utilisateurs, que ce soit leur satisfaction et leur intention d'utiliser ces mesures. Les entretiens menés précédemment montrent que les mesures imposées impactent l'intention d'utilisation et la satisfaction de certains utilisateurs quand ces mesures sont trop restrictives et

augmentent de manière trop conséquente le temps d'utilisation du SI pour réaliser les mêmes tâches qu'avant les mesures.

3.2.3. Nouveau métier : « analyste incognito »

Un phénomène que l'on observe dans de nombreux pans de la société est la tendance à embellir la réalité auprès des supérieurs hiérarchiques ou toutes personnes à qui on doit d'une certaine manière rendre des comptes. On le constate aussi dans l'expérience menée dans ce mémoire avec le questionnaire, où c'est par de multiples questions qu'on obtient une vision plus proche de la réalité que celle initialement annoncé par les répondants qui se considéraient quasiment tous comme des personnes respectant les règles de sécurité de leur entreprise.

Une émission de « télé-réalité » nommé « Patron incognito », adaptée du programme britannique « Undercover boss » trouve son concept dans le fait qu'une personne avec un haut poste dans une entreprise s'infiltre auprès d'employés « lambda ». Pour cela, il se fait déguiser pour ne pas être reconnu, avec divers prétextes comme par exemple être présenté comme une personne en recherche d'emploi qui fait des stages de découvertes, dans le but de déceler les défauts de l'entreprise, en étant sur le terrain, afin d'y remédier.

C'est de cette émission et de mes expériences professionnelles que m'est venu l'idée suivante.

Un prestataire, qui serait présenté comme un stagiaire, un apprenti ou même un nouvel employé serait formé par du personnel afin de se rendre compte de comment les utilisateurs utilisent les systèmes d'information. Cela pour se rendre compte quels en sont les problèmes de sécurité et d'expérience utilisateur. En effet, lors de mes différents stages et apprentissages, on m'a souvent mis en avant les points négatifs, avec les outils à utiliser en théorie et comment finalement passer outre ces outils qui sont jugés n'étant pas suffisamment performant. Les personnes sont plus susceptibles de dire leur fond de pensée sans filtre à une personne inférieure dans l'échelle hiérarchique qu'à un supérieur hiérarchique.

3.3. Limites et perspectives

Le résultat de cette étude reste peu significatif et demande des travaux supplémentaires. La nature même d'un système d'information, qui comme son nom l'indique, est un système résultant d'un tout. Ce tout est composé d'éléments techniques et sociaux, qui eux-mêmes contiennent de nombreuses de disciplines.

Ainsi, pour pouvoir estimer la surface d'attaque humaine, il faut s'intéresser à l'individu, seul, avec ses propres caractéristiques, mais aussi à l'individu dans un ensemble, que ce soit dans une équipe, dans une entreprise, dans un pays. Puis, les options permettant d'estimer cette surface d'attaque sont soumises aux limites techniques, mais surtout aux lois, que ce soit le respect du code du travail ou encore du règlement général sur la protection des données, ainsi qu'à des considérations éthiques.

Cette problématique nécessite une analyse interdisciplinaire, avec des experts en sciences comportementales (anthropologue, psychologue, neuroscientifique, etc.), en droit et en informatique (IA, big data, cybersécurité, développeur, designeur UX/UI).

Conclusion générale

L'impact du facteur humain sur la surface d'attaque est très important au vu des attaques de ces dernières années impliquant une erreur humaine. Ce mémoire tend à le montrer par les comportements dangereux que peuvent avoir les utilisateurs comme en témoigne l'enquête.

L'objectif fut surtout de proposer des esquisses de solutions à la fois dans le but de qualifier voire de quantifier cette surface d'attaque humaine, mais aussi des solutions pour la réduire.

Cet enjeu est de l'ordre des enjeux qui ont existé lors du passage des « Technologies de l'Information » (TI), essentiellement basées sur une approche technique au « système d'information » (SI) où apparait le rôle de l'organisationnel et de la stratégie, en adéquation avec les solutions techniques.

En effet, la solution à ce défi ne se trouve pas dans des solutions techniques ou des procédures et règlements concernant que le système d'information mais sur le fonctionnement même d'une entreprise.

Le ressenti des utilisateurs recueillis dans ce mémoire montre que des questions propres à l'organisation de l'entreprise, que ce soit par exemple par le manque de personnel, des délais restreints, des outils inadaptés, le manque de formation ou encore le sentiment de ne pas être consulté.

C'est le sens même de la dernière version du modèle de succès des systèmes d'information avec des variables indépendantes qui sont notamment liées à l'environnement professionnel plus qu'au fonctionnement des systèmes d'information. La surface d'attaque humaine est intrinsèquement liée à ces variables indépendantes et nous devons nous demander comment repenser nos organisations contre le risque de subir une cyberattaque.

Aussi, le modèle d'acceptation des nouvelles technologies est crucial pour déployer des solutions de sécurité réellement utilisées par les utilisateurs sans que cela ait un impact négatif.

Enfin, pour le cas de la France, on peut s'interroger sur le rôle du comité social et économique qui pourrait permettre la mise en pratique des théories comme celles du modèle de succès des systèmes d'information et du modèle d'acceptation des nouvelles technologies.

Depuis 2017, le CSE succède notamment au comité d'hygiène, de sécurité et des conditions de travail (CHSCT) dont le sens du mot sécurité pourrais très bien prendre la question de la sécurité des systèmes d'information Cela permettrait de définir des mesures en accord avec les représentants du personnel pour qu'elles soient plus respectées, acceptées (TAM) et plus efficaces, permettant le succès du SI (ISSM).

Bibliographie

Agarwal, R., & Prasad, J. (1997). *The Role of Innovation Characteristics and Perceived Voluntariness in the Acceptance of Information Technologies*. 26.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179-211. https://doi.org/10.1016/0749-5978(91)90020-T

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security*, *26*(4), 276-289. https://doi.org/10.1016/j.cose.2006.11.004

ANSSI. (2022). *Attaque par hameçonnage (phishing)*. ANSSI. https://www.ssi.gouv.fr/entreprise/principales-menaces/cybercriminalite/attaque-par-hameconnage-phishing/

***Attack Surface Analysis—OWASP Cheat Sheet Series*. (2022)**. https://cheatsheetseries.owasp.org/cheatsheets/Attack_Surface_Analysis_Cheat_Sheet.html

Benbasat, I., & Barki, H. (2007). Quo vadis TAM? *Journal of the association for information systems*, *8*(4), 7.

Blythe, M., Petrie, H., & Clark, J. A. (2011). F for fake : Four studies on how we fall for phish. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 3469-3478. https://doi.org/10.1145/1978942.1979459

CESIN. (2022). *Baromètre de la cybersécurité des entreprises vague 7-Opinionway-CESIN_Janv2022(1).pdf*. https://www.cesin.fr/uploads/files/Barome%CC%80tre%20de%20la%20cyber

se%CC%81curite%CC%81%20des%20entreprises%20vague%207-Opinionway-CESIN_Janv2022(1).pdf

Chiew, K. L., Yong, K. S. C., & Tan, C. L. (2018). A survey of phishing attacks : Their types, vectors and technical approaches. *Expert Systems with Applications*, *106*, 1-20. https://doi.org/10.1016/j.eswa.2018.03.050

CLUSIF. (2022). *Phishing*. https://clusif.fr/. https://clusif.fr/glossaire/phishing/

CNIL. (2022). *Le phishing, c'est quoi ?* | *CNIL*. https://www.cnil.fr/fr/cnil-direct/question/le-phishing-cest-quoi

Costa, P. T., Terracciano, A., & McCrae, R. R. (2001). Gender differences in personality traits across cultures : Robust and surprising findings. *Journal of Personality and Social Psychology*, *81*(2), 322-331. https://doi.org/10.1037/0022-3514.81.2.322

Cybermalveillance. (2022). *Que faire en cas de phishing ou hameçonnage ?* Assistance aux victimes de cybermalveillance. https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/hameconnage-phishing

Davis, F. D. (1985). *A technology acceptance model for empirically testing new end-user information systems : Theory and results*.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User Acceptance of Computer Technology : A Comparison of Two Theoretical Models. *Management Science*, *35*(8), 982-1003. https://doi.org/10.1287/mnsc.35.8.982

DeLone, W. H., & McLean, E. R. (1992). Information Systems Success : The Quest for the Dependent Variable. *Information Systems Research*, *3*(1), 60-95. https://doi.org/10.1287/isre.3.1.60

DeLone, W. H., & McLean, E. R. (2003). The DeLone and McLean model of information systems success : A ten-year update. *Journal of management information systems*, *19*(4), 9-30.

DeLone, W. H., & McLean, E. R. (2016). Information Systems Success Measurement. *Foundations and Trends® in Information Systems*, *2*(1), 1-116. https://doi.org/10.1561/2900000005

Diaz, A., Sherman, A. T., & Joshi, A. (2018). *Phishing in an Academic Community : A Study of User Susceptibility and Behavior* (arXiv:1811.06078). arXiv. http://arxiv.org/abs/1811.06078

Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006). Decision strategies and susceptibility to phishing. *Proceedings of the Second Symposium on Usable Privacy and Security - SOUPS '06*, 79. https://doi.org/10.1145/1143120.1143131

Fishbein, M., & Ajzen, I. (1975). *Belief, Attitude, Intention, and Behavior : An Introduction to Theory and Research.* Addison-Wesley. http://people.umass.edu/aizen/f&a1975.html

Flament, C. (1962). L'analyse de similitude. *Cahiers du Centre d'Études de Recherche Opérationnelle*, *4*, 63-97.

Flament, C. (1981). L'analyse de similitude : Une technique pour les recherches sur les représentations sociales. *Cahiers de Psychologie Cognitive/Current Psychology of Cognition*.

Geneiatakis, D. (2016). Minimizing Databases Attack Surface Against SQL Injection Attacks. In S. Qing, E. Okamoto, K. Kim, & D. Liu (Éds.), *Information and Communications Security* (p. 1-9). Springer International Publishing. https://doi.org/10.1007/978-3-319-29814-6_1

Ghasemshirazi, S., & Heydarabadi, P. (2021). *Exploring the Attack Surface of WebSocket*. 5.

Greitzer, F. L., Li, W., Laskey, K. B., Lee, J., & Purl, J. (2021). Experimental Investigation of Technical and Human Factors Related to Phishing Susceptibility.

ACM Transactions on Social Computing, *4*(2), 1-48. https://doi.org/10.1145/3461672

Halevi, T., Lewis, J., & Memon, N. (2013). *Phishing, Personality Traits and Facebook* (arXiv:1301.7643). arXiv. http://arxiv.org/abs/1301.7643

Hartwick, J., & Barki, H. (1994). Explaining the Role of User Participation in Information System Use. *Management Science*, *40*(4), 440-465. https://doi.org/10.1287/mnsc.40.4.440

Insee. (2022). *En 2020, l'emploi continue d'augmenter dans la fonction publique, notamment dans le versant hospitalier—Insee Première—1897*. https://www.insee.fr/fr/statistiques/6215551

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, *50*(10), 94-100. https://doi.org/10.1145/1290958.1290968

Lastdrager, E. E. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science*, *3*(1), 9. https://doi.org/10.1186/s40163-014-0009-y

Li, W., Lee, J., Purl, J., Greitzer, F., Yousefi, B., & Laskey, K. (2020). *Experimental Investigation of Demographic Factors Related to Phishing Susceptibility*. Hawaii International Conference on System Sciences. https://doi.org/10.24251/HICSS.2020.274

Lin, T., Capecci, D. E., Ellis, D. M., Rocha, H. A., Dommaraju, S., Oliveira, D. S., & Ebner, N. C. (2019). Susceptibility to Spear-Phishing Emails : Effects of Internet User Demographics and Email Content. *ACM Transactions on Computer-Human Interaction*, *26*(5), 1-28. https://doi.org/10.1145/3336141

Manadhata, P. K., Tan, K. M., Maxion, R. A., & Wing, J. M. (2007). *An Approach to Measuring a System's Attack Surface:* Defense Technical Information Center. https://doi.org/10.21236/ADA476977

Marchand, P., & Ratinaud, P. (2011). *L'analyse de similitude appliquée aux corpus textuels : Les primaires socialistes pour l'élection présidentielle française (septembre-octobre 2011)*. 13.

McCrae, R. R., & Costa, P. T. (2008). *The Five--Factor Theory of Personality*. 23.

Meurant, S., & Cardon, R. (2021). *RAPPORT D'INFORMATION FAIT au nom de la délégation aux entreprises relatif à la cybersécurité des entreprises*. http://www.senat.fr/rap/r20-678/r20-6781.pdf

Mohebzada, J. G., Zarka, A. E., Bhojani, A. H., & Darwish, A. (2012). Phishing in a university community : Two large scale phishing experiments. *2012 International Conference on Innovations in Information Technology (IIT)*, 249-254. https://doi.org/10.1109/INNOVATIONS.2012.6207742

Montesdioca, G. P. Z., & Maçada, A. C. G. (2015). Measuring user satisfaction with information security practices. *Computers & Security*, *48*, 267-280. https://doi.org/10.1016/j.cose.2014.10.015

Moore, G. C., & Benbasat, I. (1991). Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information systems research*, *2*(3), 192-222.

Petter, S., DeLone, W., & McLean, E. R. (2013). Information Systems Success : The Quest for the Independent Variables. *Journal of Management Information Systems*, *29*(4), 7-62. https://doi.org/10.2753/MIS0742-1222290401

Pitt, L. F., Watson, R. T., & Kavan, C. B. (1995). Service Quality : A Measure of Information Systems Effectiveness. *MIS Quarterly*, *19*(2), 173. https://doi.org/10.2307/249687

Rhee, H.-S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security : Its influence on end users' information security practice behavior. *Computers & Security*, *28*(8), 816-826. https://doi.org/10.1016/j.cose.2009.05.008

Rogers, E. M., Singhal, A., & Quinlan, M. M. (2014). Diffusion of innovations. In *An integrated approach to communication theory and research* (p. 432-448). Routledge.

Seddon, P. B. (1997). A Respecification and Extension of the DeLone and McLean Model of IS Success. *Information Systems Research*, *8*(3), 240-253. https://doi.org/10.1287/isre.8.3.240

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? : A demographic analysis of phishing susceptibility and effectiveness of interventions. *Proceedings of the 28th International Conference on Human Factors in Computing Systems - CHI '10*, 373. https://doi.org/10.1145/1753326.1753383

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Anti-Phishing Phil : The design and evaluation of a game that teaches people not to fall for phish. *Proceedings of the 3rd Symposium on Usable Privacy and Security - SOUPS '07*, 88. https://doi.org/10.1145/1280680.1280692

Stanton, J. M., Mastrangelo, P. R., Stam, K. R., & Jolton, J. (2004). Behavioral Information Security : Two End User Survey Studies of Motivation and Security Practices. *New York*, 8.

Theisen, C., Munaiah, N., Al-Zyoud, M., Carver, J. C., Meneely, A., & Williams, L. (2018). Attack surface definitions : A systematic literature review. *Information*

and Software Technology, *104*, 94-103. https://doi.org/10.1016/j.infsof.2018.07.008

Venkatesh, Morris, Davis, & Davis. (2003). User Acceptance of Information Technology : Toward a Unified View. *MIS Quarterly*, *27*(3), 425. https://doi.org/10.2307/30036540

Venkatesh, V., & Davis, F. D. (2000). A Theoretical Extension of the Technology Acceptance Model : Four Longitudinal Field Studies. *Management Science*, *46*(2), 186-204. https://doi.org/10.1287/mnsc.46.2.186.11926

Vergès, P., & Bouriche, B. (2001). L'analyse des données par les graphes de similitude. *Sciences humaines*, 1-90.