Mémoire de Master pour l'Obtention du Master Sciences du Management

L'impact de la politique de sécurité du système d'information sur l'organisation de l'entreprise

Nicolas TOURRETTE

Tuteur universitaire
Dr Frédéric LASSALLE

Tuteur professionnel
Théault GARRIDO
SOC – EDF

Université de Bourgogne – Année universitaire 2020-2021
IAE Dijon
Master 2 Management et Administration des entreprises

Table des matières

Remerciements

Je voudrais en tout premier lieu remercier l'ensemble des professeurs du Master Sciences de Gestion, mention Management et Administration des Entreprises, pour leurs cours très formateurs et intéressants de cette année, et de leur implication dans leurs enseignements malgré les contraintes difficiles auxquelles ils ont dû faire face.

Ensuite, je voudrais remercier le directeur de ce mémoire, le docteur Frédéric LASSALLE, pour ses conseils et sa disponibilité pour la rédaction de ce travail de recherche.

Mes remerciements vont aussi à mon tuteur de stage professionnel, M. Théault GARRIDO, expert SIEM chez EDF, pour son encadrement toujours bienveillant, sa disponibilité pour répondre à mes questions ainsi que ses précieux conseils sur l'organisation de la PSSI d'entreprise chez EDF.

J'aimerais aussi remercier ma famille, et particulièrement mes parents et mon épouse, pour leur soutien, leur relecture et leurs conseils.

1 Introduction

La place des systèmes d'information dans les entreprises est devenue de plus en plus importante au fil du temps. On peut même dire qu'aujourd'hui, le système d'information y occupe une place centrale puisque tout est numérisé. En effet, l'ensemble des informations de l'entreprise sont renfermées dans son système d'informations. On peut citer de très nombreux exemples comme le système comptable, celui qui gère les finances de l'entreprise, les fichiers clients ou fournisseurs, et encore les logiciels de gestion de ressources humaines. Ces quelques exemples prouvent bien que le système d'information joue et occupe un rôle central dans son fonctionnement.

On peut d'ailleurs voir à quel point il est important car son organisation est souvent calquée sur celle de l'entreprise qu'il supporte. En effet, on retrouve généralement une part importante du système d'information dédiée à telle ou telle branche de l'entreprise, ou à une fonction spécifique. Par exemple, la partie « ressources humaines » n'occupe pas la même partie du système d'information que la partie « financière » ou encore la partie « commerciale ».

Cette importance du système d'information dans l'entreprise a des conséquences sur celle-ci. On a pu l'observer pendant ces périodes de confinement car le télétravail s'est énormément développé. C'est pourquoi beaucoup de choses ont dû se mettre en place au niveau de ce système d'information afin qu'il puisse continuer à être opérationnel, et ce même depuis l'extérieur, sans que la bonne marche de l'entreprise n'en soit affectée. Cette période a d'ailleurs été révélatrice sur l'importance vitale pour les organisations de leur système d'information, de sa disponibilité, sa sécurité et sa confidentialité.

De nombreuses attaques ont été menées à l'encontre des divers systèmes d'information propres à chaque structure. On a pu voir que le secteur de la santé était tout aussi ciblé que les autres durant cette période, malgré la nécessité évidente (pour le bon sens commun, et dont les attaquants auraient pu avoir besoin) de ce service, et ce à l'échelle nationale, internationale et mondiale. Les entreprises de ce secteur ont dû faire face à des attaques assez virulentes à l'encontre de leur système d'information. Il peut y avoir plusieurs raisons à cela. On en citera seulement ici quelques-unes afin de pouvoir montrer l'importance que cela peut avoir.

Les attaques cyber-malveillantes ont eu une part importante dans la vie des entreprises, notamment avec de nombreuses campagnes de *phishing* (ou hameçonnage en français) et de la diffusion des logiciels malveillants. Ces attaques, notamment dans la santé, pouvaient avoir (et ont toujours) certains objectifs, surtout quand elles sont opérées par des organisations concurrentes.

Parmi ces objectifs, on peut, sans trop se tromper, dire que l'espionnage est une première raison à la création d'une attaque. En effet, le but est de pénétrer dans le système d'information de l'entité ciblée afin d'avoir accès à des informations sensibles pour se les approprier. On peut notamment penser à la course aux vaccins, et même si les données concernant les grands groupes pharmaceutiques sont restées inaccessibles au public, il n'y a aucune raison pour que les centres des opérations de sécurité (SOC) de ces entreprises n'aient pas été confrontés à des menaces de ce type.

On peut également citer les attaques visant à verrouiller complètement le système d'information de l'entreprise attaquée afin d'exiger une rançon. Le prix moyen payé en 2020 s'élève à 312 493 dollars d'après un rapport de la société Palo Alto, spécialisée dans les solutions de sécurité comme les pares-feux, sur les zones Europe, États-Unis et Canada (Alric, 2021). La société Sophos, elle aussi très implantée dans la cybersécurité des entreprises, annonce une somme un peu moins pessimiste, s'élevant tout de même à près de 170 000 dollars (soit 142 000 euros) pour la moyenne mondiale (Sophos, 2021). Certaines organisations témoignent d'ailleurs (sous couvert de l'anonymat) de sommes

versées bien plus importantes, de l'ordre de dix millions de dollars, par exemple dans la santé.

Ces quelques exemples montrent bien l'importance capitale que prend le système d'information dans la bonne marche des affaires de l'entreprise, ou de n'importe quelle autre organisation, quelle qu'elle soit. Et on mesure aussi l'absolue nécessité qu'a ce système d'information d'être sécurisé. En effet, on en revient toujours à ce problème : pour fonctionner correctement et offrir convenablement ses services, un système d'information doit être sécurisé.

Cette sécurisation passe par un élément-clé dans toutes les entreprises qui veulent assurer au mieux la sécurité et la disponibilité de leurs données. Cet élément est nommé « politique de sécurité du système d'information » et souvent abrégé par le sigle PSSI. On reviendra dans un prochain chapitre sur tous les éléments constitutifs d'une PSSI et on en présentera les tenants et les aboutissants afin de bien comprendre son rôle.

À partir de tous ces éléments introductifs, ce mémoire s'intéressera au rôle que peut jouer la PSSI dans l'organisation de l'entreprise. En effet, on peut déjà dire que cette politique, bien entendu, est interne et propre à chaque entreprise, qui la définit et la met en œuvre selon sa propre logique. Chaque entreprise étant différente, elle aura besoin d'aborder des problèmes qui lui sont spécifiques en matière de cybersécurité.

Comme dit précédemment, le télétravail généralisé depuis un an a contraint également les organisations en place à évoluer et à aborder différemment les problèmes, notamment parce qu'il en a créé de nouveaux. L'absence d'articles de recherche très précis sur le sujet nous empêche d'aborder cette partie, mais cela fait partie intégrante du problème et doit tout de même être intégré dans la conception de la PSSI.

On traitera donc ici la partie concernant la politique de sécurité du système d'information et son impact sur l'organisation de l'entreprise en répondant à la problématique suivante : « *Pourquoi la politique de sécurité du système*

d'information d'une organisation impacte-t-elle directement son mode de fonctionnement ? »

Dans un premier temps, on s'intéressera à des considérations générales sur la politique de sécurité d'un système d'information en définissant ce qu'est cette politique, son rôle et sa raison d'être, ainsi que des concepts généraux sur son élaboration et sur les acteurs indispensables. Dans une seconde partie, on s'intéressera aux différents impacts de la politique de sécurité du système d'information sur l'entreprise : impacts sur l'organisation de la hiérarchie mais aussi sur le management des collaborateurs.

2 Politique de sécurité du système d'information

Dans cette première partie, sont présentés les éléments clés qui définissent la politique de sécurité du système d'information. En effet, il faut bien comprendre les enjeux auxquels doit répondre précisément cette politique afin de pouvoir en étudier les impacts sur l'organisation de l'entreprise. Cela sera traité dans la seconde partie. Dans un premier temps, nous aborderons la définition de la politique de sécurité d'un système d'information ainsi que son rôle et sa raison d'être au sein de l'entreprise. Nous verrons ensuite quels sont les concepts clés de son élaboration et les acteurs qui seront impliqués. Enfin, on terminera par présenter les facteurs susceptibles de modifier les orientations données à la PSSI.

2.1. Définition de la politique de sécurité d'un système d'information

2.1.1. Définition générale et éléments constitutifs

L'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) définissait en 2004 la politique de sécurité d'un système d'information (qu'on abrègera par la suite par l'acronyme PSSI), comme étant « *l'ensemble formalisé des éléments stratégiques, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection du système d'information de l'organisme* » (Agence Nationale de la Sécurité des Systèmes d'Information, 2004). Cette définition a l'avantage de présenter de manière très synthétique l'ensemble des éléments constitutifs de la PSSI d'une organisation. Ainsi, on peut aisément s'apercevoir qu'il s'agit en fait moins d'un document

technique que d'un document organisationnel et stratégique. En effet, il ne s'agit pas vraiment de lister un ensemble d'éléments techniques à mettre en œuvre pour parvenir à la sécurisation du système d'information de l'entreprise. Bien sûr, cette politique contiendra, en certaines parties, des éléments techniques comme des solutions à mettre en œuvre pour répondre aux problèmes auxquels est confrontée l'entreprise (ou l'organisation de manière générale, car nous ne sommes pas forcément dans un contexte d'entreprise quand il s'agit des systèmes d'information). Elle devra aussi contenir l'ensemble des obligations, principes, règles et procédés qui favoriseront une sécurité satisfaisante des systèmes d'informations.

Cette politique va devoir s'appuyer sur un certain nombre de principes de sécurité. Ces principes sont « *l'expression des orientations de sécurité nécessaires et des caractéristiques importantes vis-à-vis de la sécurité du système d'information* » (ibid.). Pour être plus concret, un principe de sécurité peut par exemple stipuler les modalités de contrôle de l'application ou de la mise en œuvre de la PSSI au sein de l'entreprise. Un autre exemple serait d'avoir un principe de sécurité qui va définir et caractériser le niveau de confidentialité des informations.

Ensuite, il va bien sûr falloir définir les différentes règles de sécurité qui rentrent en compte dans les périmètres couverts par la PSSI visée. En effet, une entreprise peut avoir plusieurs PSSI, une par périmètre ou division. On voit donc bien que l'organisation de l'entreprise impacte la conception de la PSSI. Les règles de sécurité sont et définissent « *les moyens et les comportements pris en compte dans le cadre de la PSSI* » (ibid.). Lors de la définition de ces règles, on décline simplement les principes de sécurité établis précédemment en moyens concrets d'action. Ces règles doivent être établies pour répondre et venir encadrer les utilisateurs et les méthodes dans un environnement et un contexte donnés.

L'ANSSI rappelle bien dans ses documentations que la PSSI est un document de stratégie pour l'entreprise. En effet, il s'agit pour elle de définir les orientations stratégiques concernant la sécurité de son système d'information qui, on l'a vu,

est désormais prépondérant aujourd'hui dans ses activités. L'ANSSI précise d'ailleurs un point très important concernant la mise en place d'une telle réflexion. Elle explique que « *la PSSI traduit la reconnaissance formelle de l'importance accordée par la direction générale de l'organisme à la sécurité de son ou ses systèmes d'information* » (ibid. et repris dans Barlette, 2012). On voit donc bien l'importance d'un tel document dans l'entreprise. En effet, ce document doit être validé et approuvé au plus haut niveau de la direction pour avoir toute la portée nécessaire. Cela sera souligné davantage dans la seconde partie.

Le document de PSSI d'une entreprise prévoit donc une organisation de la sécurité du système d'information, ou seulement d'une de ses parties. En effet, on peut prendre un exemple concret. Chez EDF, puisque c'est ce qu'on a pu observer pendant le stage, il n'existe pas qu'une unique politique de sécurité, car le système d'information complet est beaucoup trop étendu. Il gère les multiples activités de l'entreprise : ressources humaines, production énergétique, facturation, applications web dédiés aux clients, etc. Ainsi, il a été décidé de découper ce système en différentes zones, en différents périmètres, auxquels s'appliquent une politique de sécurité spécifique. Ceux-ci sont en général définis par les applications. Ainsi, une application correspondra à un périmètre. Nous verrons par la suite comment ce découpage influe également dans l'organisation de l'entreprise, mais on peut déjà appréhender le lien extrêmement fort qui existe entre la manière de décider de la sécurité du système d'information et l'organisation de l'entreprise. Ce lien n'est pas forcément perceptible quand on regarde une entreprise de l'extérieur, mais il devient visible quand on commence à découper les différentes briques.

Il est aussi permis, à travers cet exemple, de remarquer le fait que le support de l'information dans l'entreprise n'est en réalité pas qu'un simple support. En effet, on peut constater que ce n'est pas si évident. On pourrait être tenté de dire de prime abord : « le système d'information est contraint par l'organisation de l'entreprise et il doit la refléter », notamment au niveau du découpage des parties du système d'information calquées sur les différents métiers ou directions de l'entreprise. En revanche, le fait que, dans le cas d'EDF, le système d'information

ait une influence sur l'organisation de l'entreprise vient invalider cette idée préconçue qui consiste à plaquer l'organisation de l'entreprise sur le système d'information pour le structurer. En réalité, on va rapidement s'apercevoir que, lorsqu'il faut sécuriser notre système d'information, l'organisation d'entreprise pensée au départ va s'en trouver modifiée.

2.1.2. Rôle et raison d'être de la PSSI

On a disserté dans le paragraphe précédent sur la PSSI en tant que telle, et commencé à entrevoir les impacts qu'elle peut avoir, mais il faut aussi se poser la question de sa raison d'être. En effet, pourquoi les entreprises sont-elles invitées à mettre en place un tel document ? Ce document, on le rappelle, devra bien entendu avoir un impact fort et des conséquences sur la technique afin de parvenir à attendre l'objectif : la sécurisation du système d'information. La raison d'être de la PSSI de tout ou d'une partie d'un système d'information est bien de parvenir à garantir la meilleure sécurité des informations qu'il renferme. En effet, ces données sont essentielles à la vie de l'entreprise et il ne peut pas être laissé de place à une éventuelle intrusion au sein de ce système, ce qui entrainerait des conséquences assez dramatiques pour l'entreprise. On a abordé en introduction les problématiques de rançon, mais il peut bien sûr y avoir d'autres menaces : l'espionnage, l'intelligence économique, le vol de données pour la revente, la volonté de mettre en péril l'existence d'une entreprise, etc. Il faut tout de même garder à l'esprit, lors de la rédaction de ce document de stratégie qu'est la PSSI, que le risque zéro n'existe pas. La sécurité d'un système d'information ne sera jamais parfaite, quel qu'il soit, et quelle que soit la façon dont a été menée la conception et la mise en œuvre d'une politique de sécurité.

Nathalie Dagorn et Nicolas Poussing font une remarque qui va bien dans le sens de l'ANSSI et d'Yves Barlette dans leur article *Engagement et pratiques des organisations en matière de gouvernance de la sécurité de l'information* (Dagorn & Poussing, 2012). En effet, ils indiquent que 95 % des entreprises pensent tirer un bénéfice concurrentiel lorsqu'elles sont engagées dans une démarche d'élaboration de politique de sécurité du système d'information. De plus, ils

indiquent que 75 % d'entre elles sont engagées dans une telle démarche. D'après eux, les entreprises pensent pouvoir tirer profit de façon importante ou très importante de la gouvernance de la sécurité de l'information. Elles décrivent en général treize bénéfices qu'elles tirent de leur investissement dans ce domaine, et les plus importants sont l'amélioration des procédures en matière de sécurité, la conformité avec la législation (d'où l'importance de l'étude du cadre réglementaire décrite dans le prochain paragraphe) et la confiance augmentée des partenaires. On constate donc bien une fois de plus que la sécurité du système d'information est un enjeu stratégique pour l'entreprise, et bien qu'elle mette en jeu des composantes techniques (il faut bien assurer la sécurisation d'une manière concrète), le premier enjeu de l'élaboration d'une PSSI n'est pas la technique mais bien les orientations et l'inscription dans un contexte stratégique et organisationnel.

2.2. Concepts clés de l'élaboration d'une politique de sécurité d'un système d'information

Après avoir défini et cerné le rôle de la politique de sécurité du système d'information en entreprise, nous allons voir comment celle-ci est élaborée. Pour mieux comprendre ce processus de conception, nous allons détailler les concepts clés de l'élaboration de ce document. Nous n'aborderons pas l'aspect technique que peut constituer un tel document pour nous concentrer uniquement sur les concepts clés axés sur les sciences de gestion.

2.2.1. Dimensions essentielles

Tout d'abord, il faut rappeler les quatre dimensions sur lesquelles s'appuie une PSSI.

En premier lieu, il y a une dimension juridique. En effet, une PSSI s'inscrit forcément dans le cadre juridique du pays dans lequel elle va être appliquée, et on en perçoit la teneur avec l'entrée en vigueur du règlement européen général sur la protection des données (RGPD) le 25 mai 2018. Les entreprises ont désormais de nouvelles règles concernant la collecte et l'exploitation des

données des utilisateurs, et le système d'information ne fait pas exception à la règle. Donc si certains outils permettant de garantir la sécurité du système d'information ou bien permettant d'en surveiller la qualité sont mis en œuvre dans le cadre de cette politique, alors des lois vont venir régir l'utilisation que l'entreprise pourra en faire. Yves Barlette le souligne également dans *Implication et action des dirigeants : quelles pistes pour améliorer la sécurité de l'information en PME ?* quand il dit qu'il « *existe de nombreuses réglementations ayant des rapports avec la SSI : une des plus connues est la loi informatique et libertés (CNIL) qui va engager la responsabilité pénale du dirigeant afin d'éviter que les informations nominatives gérées par l'entreprise soient "déformées, endommagées ou communiquées à des tiers non autorisés"* » (Barlette, 2012). Il existe aussi de nombreuses autres contraintes réglementaires en termes de sécurité des systèmes d'information en fonction du secteur d'activité dans lequel s'est positionnée l'entreprise (banque, santé, etc.).

Ensuite, on a une dimension organisationnelle car il est bien évident que la PSSI va venir impacter l'organisation de l'entreprise. Cette partie sera donc beaucoup plus développée par la suite et nous ne nous n'y attarderons pas davantage pour le moment. L'autre composante qui va de pair avec celle-ci est la dimension économique. Les impacts organisationnels de la PSSI vont aussi avoir des impacts sur les performances économiques car elle peut alourdir les coûts, ou bien au contraire prévenir des attaques de cybersécurité, et ainsi faire gagner beaucoup à l'entreprise. Yves Barlette le souligne rapidement en disant que la Direction doit jouer un rôle d'arbitrage entre la mise en œuvre de la SSI et les pertes possibles de productivité (Barlette, 2012). En effet, le fait d'affecter des ressources humaines sur le projet d'élaboration de la PSSI peut conduire à une baisse de ressources pour les autres activités opérationnelles, et donc engendrer des pertes. En revanche, la Direction doit correctement réaliser son arbitrage afin de gérer au mieux ce projet.

En dernier point, on note les deux dimensions technique et humaine. Ces deux dimensions sont aussi à prendre en compte car le facteur technique rentre forcément en ligne de jeu assez rapidement quand on propose des concepts et

des règles de sécurité. Il faut que la politique reste réaliste et il est inutile de prévoir des actions qui sont techniquement infaisables ou qui exigeraient un budget colossal.

De plus, le facteur humain est également déterminant, car il faudra non seulement former les salariés et autres personnes intervenant dans l'entreprise à la politique de sécurité, mais également surveiller si leurs actions sont bien conformes aux règles définies par la PSSI. Pour cela, il faut s'assurer que les utilisateurs aient bien compris les tenants et aboutissants de la politique, que ses objectifs soient suffisamment clairs, et que les utilisateurs du système d'information puissent voir l'intérêt de telle ou telle règle afin d'y adhérer et donc de les respecter. On constate, en général, que les utilisateurs ne respectent que les règles qu'on leur a expliquées et qu'ils ont comprises. Il faut donner un sens concret à cette PSSI facilement perceptible par les salariés de l'entreprise.

2.2.2. Phases de l'élaboration

L'élaboration de la PSSI se décompose en quatre phases bien distinctes. De plus, ces phases sont interdépendantes, c'est-à-dire qu'on ne peut passer à la phase suivante que si la phase en cours est complètement achevée et validée. En effet, les éléments utilisés dans chaque phase s'appuient sur les étapes précédentes. On peut donc dire que la conception d'une PSSI est similaire à un exercice en tiroirs dans lequel le succès pour répondre à la question $n+1$ est d'avoir correctement répondu à la question n. En revanche, cet exemple simple pour illustrer le fonctionnement de l'élaboration de la PSSI n'est vrai que pour l'enchaînement des tâches : il n'y a pas de bonnes ou mauvaises façons d'aborder chaque étape. Si l'on veut comparer le processus d'élaboration à un concept plus théorisé en sciences de gestion, on peut prendre l'élaboration d'un planning représenté par un diagramme de Gantt, avec des jalons à valider, et sans lesquels on ne peut passer à l'étape suivante.

2.2.2.1. Phase initiale : préparation du projet de PSSI

La toute première étape est la phase initiale ou dite « préparatoire ». Cette phase a pour but de définir les objectifs et les moyens à mettre en œuvre lors de l'élaboration de la PSSI. C'est le tout début du chantier d'élaboration et cette phase s'organise comme cela pourrait être fait lors des réunions de préparation d'un projet. L'équipe en charge de l'élaboration de la politique définit clairement les objectifs, définit et met en place les indicateurs permettant de suivre le projet, construit les tableaux de bord associés. Cette équipe est dirigée par un chef de projet ou bien directement par le responsable de la sécurité du système d'information (RSSI).

Une fois cette première étape effectuée, l'équipe projet peut alors réfléchir et définir le cadre documentaire de la PSSI et ses grandes lignes. Il doit recenser les aspects légaux et réglementaires (par exemple dans le cas de l'application du RGPD, de la loi de confiance pour l'économie numérique, dite LCEN, ou la loi de programmation militaire, dite LPM, pour les OIV[1]). Le cadre documentaire doit aussi indiquer les grands principes d'éthique, les obligations contractuelles auxquelles l'entreprise s'est engagée, les obligations contractuelles des prestataires et des partenaires ainsi que le référentiel de sécurité interne. Ce référentiel est un document visant à renforcer la confiance des utilisateurs du système d'information dans les services proposés par celui-ci. Il peut également être vu comme un référentiel des bonnes pratiques en matière de sécurité du système d'information.

Tout ceci donne lieu à la constitution d'un document appelé « note de cadrage ». Il a pour but de reprendre les éléments précités, et de constituer le cahier des charges pour le projet d'élaboration de la PSSI d'une partie ou de tout le système d'information suivant le périmètre étudié. On peut aussi y trouver des documents plus techniques comme les analyses de risques, ou bien des résultats d'audits de sécurité, qui ont été réalisés pour donner une vision d'ensemble sur les

[1] Organisme d'importance vitale : organisme indispensable à la survie de l'État et de la Nation en temps de crise grave.

risques encourus par le système d'information et les éventuelles failles qui y sont présentes au début du projet.

Il est important de noter l'importance de cette phase préparatoire qui va déterminer en grande partie le respect des échéances fixées par le projet, permettre d'examiner les différentes pistes dans des délais raisonnables et de prévoir en amont un certain nombre de cas possibles.

2.2.2.2. Phase d'élaboration des éléments stratégiques

Durant cette seconde phase, les éléments stratégiques déterminants de la PSSI vont être déterminés avec précision. En effet, c'est lors de cette phase qu'il faut décider du périmètre de surveillance de la PSSI : va-t-elle concerner l'ensemble du système d'information ou bien seulement à une application, ou encore à une partie de l'entreprise (par exemple la partie « Commerce » ou « Ressources Humaines ») ? Cette focalisation va permettre de couvrir un enjeu stratégique commun à de nombreuses entreprises : avoir la meilleure performance opérationnelle. Ainsi, lors de la réalisation du projet, les coûts financiers et humains seront réduits car les périmètres auront été ciblés avec précision, et même en amont de cela, le projet sera davantage focalisé sur l'atteinte des bons objectifs sans s'être dispersé. Là encore, la performance dans la réalisation du projet d'élaboration de la PSSI sera meilleure.

Lors de cette phase, il faut aussi se concentrer à la classification des équipements et des besoins afin de déterminer avec précision le degré de sécurisation à apporter à chaque niveau, et des besoins qui sont nécessaires et suffisants, que ce soit par les équipes techniques ou bien les métiers. Cela passe notamment par le discernement et l'analyse des enjeux de sécurité pour l'entreprise, et par l'identification des infrastructures ou des services critiques pour la bonne marche de l'entreprise. Si l'on peut prendre un exemple ici, un système de facturation ou de gestion des commandes sera jugé critique tandis qu'un serveur de fichiers le sera beaucoup moins. L'étude des menaces potentielles est elle aussi très importante et va permettre de cibler et qualifier davantage le degré de sécurisation recherché précédemment.

Avec tous ces éléments, on peut désormais réfléchir à la stratégie générale que devra adopter la PSSI tout en respectant le cadre documentaire et réglementaire défini lors de la première phase. On peut d'ores et déjà penser aux principes de sécurité que nous voulons mettre en œuvre avec cette politique.

Le document résultant de cette phase est une note de stratégie de sécurité. Cette note doit être présentée à la Direction générale de l'entreprise afin de valider les orientations stratégiques que l'on y a définies. On voit bien que la PSSI est alors plus un document de stratégie pour l'entreprise qu'un document technique. Ce point est très bien mis en exergue dans l'article *Implication et action des dirigeants : quelles pistes pour améliorer la sécurité de l'information en PME ?* publié par Yves Barlette en 2012 (Barlette, 2012). En effet, il insiste fortement dans son article sur l'importance du fait que la PSSI doit « *être considérée comme un problème de gestionnaire et non de technicien* » (voir aussi Barlette, 2008).

2.2.2.3. Phase de sélection des principes et de rédaction des règles

Après avoir réfléchi et pensé la PSSI, l'entreprise, et particulièrement l'équipe projet qui en est responsable, va pouvoir rédiger le document de politique de sécurité à proprement parler. Ce document devra reprendre les choix stratégiques faits en termes de sécurité, et dictera l'ensemble des règles applicables afin de garantir ceux-ci. On aboutira dans cette phase à la rédaction d'une première note de synthèse justifiant des choix des différentes règles inscrites à la PSSI et d'une seconde détaillant les impacts organisationnels et financiers.

Pour cela, il faudra choisir dans un premier temps les principes de sécurité que l'entreprise veut mettre en place. Ce choix va s'effectuer sur la base des éléments élaborés précédemment : le référentiel du système d'information (à l'aide de la note de cadrage rédigée dans la phase initiale), la définition du périmètre de la PSSI, la liste des besoins de sécurité identifiés et la liste des origines des menaces retenues et des risques (tout cela se trouve dans la note stratégique de sécurité rédigée lors de la phase précédente). On voit donc bien que sans avoir

validé les précédents jalons, la rédaction de la PSSI devient impossible. Par la suite, on formulera les consignes à respecter afin de mettre en œuvre les principes de sécurité qui ont été rédigés.

2.2.2.4. Phase de finalisation et de validation

Cette dernière phase vient clôturer le cycle d'élaboration de la PSSI. En effet, la relecture du document, sa validation et sa signature par la Direction de l'entreprise sont les composantes principales de cette phase. La relecture et la validation permettent de vérifier la cohérence et l'atteinte de l'exhaustivité recherchée dans les différentes règles énoncées. La signature vient appuyer et soutenir la stratégie définie dans la PSSI ainsi que l'ensemble des moyens organisationnels, techniques et humains et managériaux qui seront mis en œuvre lors du déploiement de la politique. On établira également un plan d'action qui prévoira ce déploiement. Il faut bien sûr prévoir de former le personnel à ces nouvelles thématiques et aux moyens de mise en œuvre concrets de cette politique. Cela aura pour objectif principal de déployer sereinement la politique sur le périmètre concerné et de minimiser les pertes et impacts néfastes durant cette phase de mise en place. Ce plan d'action présentera la politique rédigée aux collaborateurs afin d'expliquer tous les principes et règles définis, leur moyen d'application et les impacts sur l'entreprise.

2.3. Facteurs pouvant modifier l'orientation donnée à la PSSI

Après avoir parcouru les différentes phases de l'élaboration de la PSSI et ses concepts clés, il nous faut maintenant discuter sur les facteurs principaux pouvant modifier l'orientation qui sera donnée à la politique de sécurité. Cette partie n'a pas vocation à être exhaustive car le champ de la recherche n'est pas suffisamment développé pour ce faire. De plus, il serait prétentieux de faire une liste complète des facteurs influençant cette élaboration étant donné que la PSSI est déjà un document propre au contexte de chaque entreprise. Nous n'en verrons donc que quelques-uns dans le cadre de ce mémoire.

2.3.1. Influence de l'implication de la Direction sur la PSSI

Pour commencer, il faut noter que, dans la majorité des articles publiés sur le sujet de la sécurité de la donnée en entreprise, un premier facteur est désigné comme crucial à l'élaboration d'une bonne politique de sécurité de la donnée. Ce facteur est l'implication du dirigeant (dans le cas d'une PME) ou de la Direction (pour une entreprise de plus grande envergure) dans les processus d'élaboration qu'on a décrit dans la partie 2.2.2. C'est notamment Yves Barlette, Nathalie Dagorn et Nicolas Poussing qui traitent de cette influence majeure dans leurs articles (Barlette, 2012; Dagorn & Poussing, 2012). En effet, ils développent l'importance de l'implication du dirigeant dans l'élaboration de la PSSI. N. Dagorn et N. Poussing rappelle dans l'introduction de leur article que la mise en place d'une PSSI et son élaboration « *impose une gestion des risques et une prise en compte des questions de sécurité de l'information au plus haut niveau de l'organisation* ». Y. Barlette renchérit quant à lui en indiquant que « *de nombreux auteurs ont déclaré que la SSI devait être prise en compte au niveau de la direction générale de l'entreprise* », citant les travaux de Markus (1983), Longeon et Archimbaud (1999), Friend et Pagliari (2000) ainsi que de Knapp *et al.* (2006). Il complète d'ailleurs bien en ajoutant que « *les dirigeants doivent donc être considérés comme le point de départ d'une mise en place d'une SSI qui puisse être considérée comme satisfaisante* ».

En effet, nous avons bien vu dans la partie traitant de l'élaboration de la PSSI au sein de l'entreprise que ce document doit faire état des enjeux majeurs de sécurité de l'information, du contexte de l'entreprise et de son secteur d'activité, des risques qu'elle doit affronter en matière de sécurité. Dans ce contexte, la Direction est particulièrement bien informée de ces éléments qui touchent de près à la santé et à la capacité de l'entreprise. Ces éléments ne sont évidemment pas à négliger, c'est pourquoi Y. Barlette appuie sur ce point en disant que pour qu'une PSSI soit satisfaisante, la Direction doit y prendre sa part. De plus, on a bien sûr pu voir que l'ANSSI préconise dans les phases d'élaboration de la PSSI une phase de validation et d'approbation de la Direction de l'entreprise. Cette politique aura des impacts forts sur son fonctionnement, comme on le verra par

la suite. La Direction doit donc donner son accord à ce « nouveau » fonctionnement, ou en tout cas à un changement dans les pratiques de l'organisation. Yves Barlette s'attache à démontrer que si le dirigeant n'est pas suffisamment impliqué dans l'élaboration de la PSSI, alors elle n'aura pas toute la portée qu'elle devrait, elle n'aura pas l'impact et les effets désirés.

Il définit l'implication comme étant « *le degré de préoccupation du dirigeant et l'importance perçue, relative au SI de son entreprise* » (Barlette, 2012). Cette implication va avoir de nombreux impacts (que nous pourrons voir par la suite), mais il est déjà utile de préciser ici que l'implication du dirigeant ne se traduit pas forcément par des actions. En effet, il se peut que le dirigeant n'ait pas (ou peu) de connaissances techniques sur la sécurité de la donnée ; les articles publiés à ce sujet vont d'ailleurs dans le sens que c'est très rarement le cas. En revanche, les dirigeants ont déjà pu vivre des expériences et voir les conséquences se rapportant à une trop faible sécurité de la donnée. Ils connaissent les risques encourus par leur entreprise vis-à-vis de ce manque.

De plus, ils ont les capacités de décider d'un budget alloué à cette tâche, à sa pérennité et à son respect dans le temps. Ils peuvent également, par leur volonté, dynamiser les équipes en charge de construire cette politique, de donner du crédit à leur travail si nécessaire, et à les guider dans l'élaboration en leur fournissant des éléments contextuels dont elles n'auraient pas connaissance. L'implication de la Direction peut aussi se faire sentir dans la façon de valider le travail fourni par l'équipe projet et le suivi qu'elle fera de sa mise en place.

En effet, si la Direction n'accorde pas visiblement d'importance à ce sujet, les équipes n'auront pas la reconnaissance de leur travail, le déploiement de la PSSI sera plus difficile, elle sera moins bien respectée par les collaborateurs. On a tous un exemple en tête d'une personne disant « si la Direction n'y accorde pas plus d'importance que cela, c'est que ce n'est pas très important pour nous ». Le célèbre proverbe « faites ce que je dis, mais pas ce que je fais » témoigne aussi de la nécessité de l'implication de la Direction dans un tel projet, même si celle-ci n'a pas forcément toutes les connaissances techniques nécessaires. En effet, ce n'est pas son travail. Sa mission est celle de s'impliquer et de reconnaître le

travail engagé, de valider correctement les propositions et de suivre avec attention le déploiement et le respect de cette politique au sein de l'organisation.

Y. Barlette donne aussi quelques détails intéressants sur les facteurs pouvant faire varier l'engagement de la Direction dans la construction de la PSSI de son entreprise. Ces éléments sont aussi des facteurs qui influencent l'orientation qui sera donnée à la PSSI. Parmi ces différents facteurs, on retrouve le passé du dirigeant (on comprendra ici « des dirigeants » s'ils sont plusieurs à prendre les décisions), l'âge, le niveau d'expérience, son ancienneté dans l'organisation ou dans sa position hiérarchique également ainsi que sa perception des opportunités et menaces en termes de sécurité de l'information. Ces facteurs entrent en ligne de compte pour l'implication du dirigeant dans le processus d'élaboration de la PSSI, comme il l'explique et le démontre dans son article. En tout cas, sa conclusion est que l'implication, *a minima* moyenne, du dirigeant est nécessaire afin de produire un travail de qualité satisfaisante pour la sécurité du système d'information. Celui-ci n'a pas besoin d'agir de manière directe ou indirecte dans l'élaboration de ce processus, mais il faut qu'il soit impliqué. Cependant, son action reste quand même nécessaire au moins lors de la dernière phase de l'élaboration puisqu'il doit valider la politique établie et la faire appliquer.

2.3.2. Les objectifs recherchés par la Direction

Un autre facteur pouvant modifier l'orientation donnée à la PSSI est celui des objectifs recherchés par la Direction. En effet, en fonction de ceux-ci, la PSSI ne va pas chercher à atteindre certains objectifs pour se concentrer sur d'autres. Comme on l'a vu, la PSSI est et reste un document stratégique. Un document stratégique a pour but de fixer certains objectifs et la manière de les atteindre. Les objectifs désirés par la Direction vont donc grandement influencer l'orientation qui sera donnée à la PSSI lors de son élaboration par l'équipe projet qui se verra confiée cette mission.

Dans leur article, Nathalie Dagorn et Nicolas Poussing définissent quelques objectifs que la Direction peut chercher à atteindre lorsqu'elle met en place une démarche de réflexion et d'élaboration de PSSI (Dagorn & Poussing, 2012).

Le premier est celui de la performance qu'elle pourra retirer de la démarche. En effet, ils ont constaté que certaines entreprises initient cette démarche afin de pouvoir en retirer une certaine valeur ajoutée et des avantages concurrentiels. Par exemple, une entreprise engagée dans une telle démarche va sans doute avoir des problèmes moins importants faces aux risques cyber ou les coûts seront peut-être réduits en cas de réussite d'une attaque car elle sera plus rapidement maîtrisée. Les équipes seront davantage préparées car la PSSI aura défini des cycles de formation ou de mise à niveau afin de garantir l'état opérationnel de réponse sur incident.

Le deuxième objectif que l'entreprise peut chercher à atteindre est celui d'améliorer la réalisation de défis. N. Dagorn et N. Poussing parlent de « *dépasser les freins et les obstacles* » (Dagorn & Poussing, 2012). Cela peut être un objectif managérial que l'entreprise se fixe pour que les équipes dépassent les difficultés qu'elles rencontrent et ainsi devenir plus performantes ou autonomes sur certains sujets sans avoir besoin de déléguer certaines tâches à des sous-traitants. Ici se superpose un objectif de réduction des coûts.

Un dernier objectif intéressant soulevé par N. Dagorn et N. Poussing est l'influence sociale que l'entreprise peut retirer de la mise en place d'une PSSI. Le déploiement d'une telle politique peut en effet profiter à l'entreprise car elle va suggérer certaines de ses valeurs. Des normes subjectives, des valeurs et une image positive peuvent alors émerger et attirer davantage l'attention sur l'entreprise, améliorer son statut au sein de son secteur d'activité… Par exemple, l'entreprise peut très bien mettre en valeur son engagement dans la sécurisation de ses données pour attirer de nouvelles compétences, suggérer son investissement dans de bonnes pratiques, influencer les autres entreprises qu'elle peut côtoyer afin de les encourager à mettre en œuvre une démarche similaire, ou même les y obliger quand il s'agit d'un groupe. Cela est assez courant : la maison mère est à l'origine d'un engagement fort dans le domaine de

la cybersécurité de ses données, et va fortement inviter (et parfois contraindre) ses filiales à instaurer des démarches similaires, cela constituant un objectif stratégique. On peut ici prendre l'exemple d'EDF qui a de nombreuses filiales non seulement en France mais aussi à l'international. EDF est engagé dans une démarche sérieuse et importante de sécurisation de son système d'information vu son importance stratégique pour la France. De plus, les filiales qui ont des connexions avec le système d'information EDF (que l'on pourrait qualifier de « père ») sont bien entendu mises au défi de mettre en œuvre des stratégies de sécurité analogues afin de ne pas compromettre ce système d'information par rebond. Le rebond désigne simplement le fait d'utiliser un système pour en atteindre un autre.

Y. Barlette donne également un objectif que peut rechercher la Direction dans l'élaboration d'une politique de sécurité pour son système d'information. Il indique que la Direction peut vouloir mettre en place une démarche d'amélioration de l'indicateur ROSI (*Return On Security Investment*) (défini notamment par le CLUSIF[2]) (Barlette, 2012). Cet indicateur met en avant des arguments technologiques, métiers, réglementaires et normatifs. Certains paramètres font écho aux propos de N. Dagorn et N. Poussing. De plus, l'amélioration de cet indicateur va permettre une meilleure gestion des crises et de limiter les impacts de celles-ci, aussi bien en termes financiers (les crises coûteront moins cher car l'entreprise se sera dotée des bonnes protections et des bonnes mesures) que marketing (l'image de l'entreprise ne sera pas dégradée à cause d'une perte des activités due à une attaque). Y. Barlette cite d'ailleurs Johnston et Hale qui ont montré que les deux premiers facteurs de prises en compte de la sécurité du système d'information par les dirigeants sont « *la nécessité de conformité avec les responsabilités civiles et pénales, suivie par l'amélioration de l'image de l'entreprise* » (Johnston & Hale, 2009).

[2] Club de la Sécurité de l'Information Français.

2.3.3. Le périmètre d'application de la PSSI

Comme il a été abordé précédemment, le périmètre d'application de la PSSI va aussi être un élément majeur dans la direction prise par la politique et le résultat final. En effet, on ne va pas aboutir au même résultat final si la PSSI s'applique uniquement à un périmètre restreint tel qu'une application, une division, ou au contraire sur le périmètre extrêmement vaste qu'est l'entreprise toute entière. Les enjeux sont différents, les personnes concernées sont autres, les systèmes informatiques mis en jeu sont distincts, les risques également, etc.

Le périmètre d'application est d'ailleurs un élément constitutif de la deuxième phase d'élaboration de la PSSI, phase portant sur les enjeux stratégiques que doit couvrir la politique. Ainsi, on peut nettement distinguer les impacts qu'ont les choix posés lors de cette étape. Si l'on reprend la comparaison de « l'exercice en tiroirs » prise pour expliquer l'emboîtement des phases d'élaboration, on peut constater que toutes les étapes suivantes se trouvent modifiées si le périmètre est différent, rendant le résultat de cette deuxième phase différent.

Si l'on peut prendre ici un exemple concret, on pourra s'appuyer sur ce qui a été observé pendant le stage. Chaque application dispose de sa propre politique de sécurité, même si l'ensemble du système d'information est contrôlé par une PSSI générale à l'entreprise. En effet, une telle granularité dans les processus de sécurisation du système d'information peut s'expliquer par les besoins spécifiques de chaque application. Est-elle à usage interne ou doit-elle être exposée sur Internet ? Qui peut y accéder ? Dans quel type d'infrastructure l'application est-elle implantée ? Y a-t-il des contraintes réglementaires ou contractuelles spécifiques à appliquer ? Qu'est-il prévu dans les *Service Level Agreements* (SLA, ou contrats de niveau de service) ? Toutes ces questions sont celles qui peuvent se poser lors de l'élaboration de la PSSI d'une application en particulier, alors qu'elles ne se poseront pas dans un contexte plus global, soit à l'échelle de la maille « division », ou à l'échelle macro du Groupe. Chez EDF vient aussi s'ajouter la dimension des interconnexions avec les filiales qui posent encore des questions plus complexes en termes de périmètre concerné car cela

nécessite d'organiser une PSSI commune entre deux entreprises régissant les flux échangés par elles sur un réseau dédié ou bien sur un réseau commun d'interconnexion, suivant par exemple le type et la criticité ou la confidentialité des données échangées par les deux entreprises. C'est aussi un cas possible dans la longue liste des périmètres de surveillance pour lesquels on peut mettre en œuvre une politique de sécurité.

2.3.4. La proportion du télétravail dans l'entreprise

Un autre facteur capable d'influencer la direction prise par la PSSI qu'élabore l'entreprise est le télétravail et sa proportion dans l'entreprise. L'article publié par Brigitte Pereira en 2018 indique que le développement des technologies de la communication et de l'information a un impact non négligeable sur l'organisation du travail (Pereira, 2018). Elle précise que cela modifie le rapport de subordination entre le salarié et l'employeur. En effet, le temps de travail devient plus adaptable et la frontière entre la vie personnelle et professionnelle devient plus floue surtout avec le télétravail (massivement développé ces derniers mois). Le salarié peut donc réfuter certaines règles de sécurité si celles-ci sont mal comprises car il n'est plus contrôlé directement par l'employeur pendant ces périodes.

Nous avons tous vécu cette période de télétravail et avons pu constater que les liens avec la hiérarchie à laquelle nous appartenons ont été transformés, plus ou moins en fonction de l'organisation, mais ce lien a évolué. Le fait d'être chez soi pour travailler peut modifier les comportements au travail, notamment l'usage que nous faisons de nos outils informatiques professionnels. Il a pu y avoir des situations dans lesquelles l'employé a probablement pu utiliser son poste de travail professionnel pour faire une recherche personnelle, passer une commande, faire une pause, ce qu'habituellement il ne fait pas au bureau, ou en tout cas pas avec le matériel fourni par l'entreprise. Ainsi, on peut dire que les changements survenus dans l'usage que nous avons des terminaux mis à disposition par l'employeur dans le cadre du télétravail nécessite l'adaptation de

la PSSI pour maîtriser les pratiques et garantir la sécurité du système d'information.

A contrario, certaines entreprises n'ont pas fourni à leurs salariés les équipements informatiques dont ils avaient besoin pour télétravailler. Ils ont donc été amenés à utiliser leurs terminaux personnels pour travailler et ainsi à accéder aux ressources de l'entreprise, avec les risques que cela comporte : diffusion de logiciels malveillants sur le système d'information, fuite d'informations confidentielles, difficulté de séparation des données personnelles et professionnelles, etc. La principale raison à cela est le fait que les terminaux personnels ne sont pas soumis au contrôle de l'employeur et difficilement atteints par les systèmes de sécurité. On voit ici ce qu'indique B. Pereira en termes de rapport employeur-employé. Ces terminaux sont donc considérés comme « à risques » pour la sécurité de l'entreprise, en tout cas dans ce contexte, mais on traitera le cas de ces équipements et de l'impact sur la PSSI ultérieurement.

On peut donc en conclure que, dans le cadre du télétravail, le pouvoir réglementaire de l'employeur est différemment perçu par les salariés et il ne peut pas être exercé de la même manière. En effet, si celui-ci permet de « *mettre en place des règles patronales ou des normes internes à l'organisation au sein de laquelle travaille le salarié* » (Pereira, 2018), le fait que les salariés soient en dehors de l'entreprise pour fournir leur activé de travail modifie ce pouvoir réglementaire. Le dirigeant contrôle donc beaucoup plus difficilement l'applications des règlements édictés du fait de l'éloignement du salarié par rapport à l'entreprise. Dans ce contexte, comment la PSSI doit-elle être rédigée et quelles orientations doit-elle prendre pour être efficace dans cette période de télétravail ? On voit donc bien que le télétravail est un facteur influent dans l'élaboration d'une PSSI robuste.

2.3.5. Les facteurs techniques

Des facteurs techniques viennent aussi orienter différemment l'élaboration de la PSSI. On a entrevu dans le paragraphe précédent le cas des terminaux personnels employés dans le cadre d'une prestation de travail pour l'entreprise.

Ce point sera repris ici avec davantage de détails, mais il existe aussi un autre facteur technique important aujourd'hui, notamment dans un contexte de souveraineté de la donnée : l'utilisation de l'open-source. Nous n'aborderons pas l'aspect technologique ici, mais bien toujours le point de vue de la science de gestion.

2.3.5.1. Le cas du BYOD

Le cas du BYOD (*bring your own device*, apportez votre propre périphérique) est un autre phénomène qui prend de plus en plus d'ampleur dans les entreprises et les universités notamment. Le principe est que chacun apporte son ordinateur ou sa tablette pour travailler. L'employeur peut subventionner une partie de l'achat ou du renouvellement du poste de travail. Cela peut aussi permettre d'augmenter le confort, la satisfaction et la productivité des salariés. En effet, certains préfèrent travailler sur tel ou tel périphérique et seront plus à l'aise car c'est un environnement qu'ils maîtrisent davantage (Mignerat, Mirabeau, & Proulx, 2019).

En revanche, cette pratique est assez difficilement contrôlable en termes de sécurité par les RSSI. Les terminaux personnels ne peuvent pas être soumis aux mêmes règles que les terminaux mis à disposition par l'entreprise, justement parce qu'ils ne lui appartiennent pas. Cet état de fait est bien souligné par Étienne Thenoz dans son article « *Gestion des usages des technologies numériques dans les organisations : une approche qualitative par le contrôle organisationnel et les chartes informatiques* ». Il faut donc trouver une réponse adaptée à cette situation afin de garantir une sécurité de la donnée d'entreprise sans avoir réellement de possibilité de contrôler techniquement le poste « BYOD » de l'utilisateur. Bien sûr, certaines techniques peuvent permettre de garantir une sécurité comme le contrôle des flux internet qui est de toute façon mis en place à l'échelle de l'organisation, mais pas directement sur les postes « BYOD », *a contrario* de ce qui peut être mis en place sur des terminaux d'entreprise (par exemple le blocage de tous les flux vers Internet si on ne passe pas par le VPN de l'entreprise).

É. Thenoz décrit quelques principes de contrôle des utilisateurs qui peuvent très bien s'appliquer à l'élaboration d'une PSSI en présence de pratiques BYOD (Thenoz, 2020). En s'appuyant sur les modes de contrôle définis par Ouchi (1979), il applique cette classification à la sécurité de la donnée en entreprise et la manière de contrôler les utilisateurs. Les directions des systèmes d'information (DSI) peuvent donc utiliser le contrôle par les comportements, par les résultats ou par la sociabilisation. É. Thenoz indique que le contrôle par les comportements s'appuie sur le principe de « *l'évaluation de la conformité du comportement* [observé] *à des règles* » (ibid.). Cette méthode de contrôle est effectivement celle employée la majeure partie du temps quand il s'agit de mettre en place des règles, des normes et des pratiques de surveillance du système d'information par des outils technologiques de contrôle. Le contrôle par résultats est plutôt orienté sur la « *mesure et l'évaluation des résultats de l'usage* » (ibid.) car on s'appuie plutôt ici sur l'analyse des résultats des pratiques informatiques en termes de performance selon différents indicateurs (il donne l'exemple de confidentialité des données ou de la compromission de la sécurité, etc.). Enfin, la dernière méthode de contrôle décrite par É. Thenoz est celle par la sociabilisation qui consiste en « *l'internalisation des normes et des valeurs de l'organisation par les utilisateurs* » (ibid.). Cette pratique s'appuie davantage sur l'intégration des bonnes valeurs par les utilisateurs qui sont davantage formés aux bonnes pratiques par l'inclusion et la motivation intrinsèque.

Au travers du travail d'É. Thenoz, on peut discerner des réponses aux problèmes rencontrés sur les orientations à donner à la PSSI dans le cas du BYOD. En effet, on a pu constater que la mise en place de règles et leur contrôle par les comportements ne seraient pas les solutions les plus adaptées. On ne dit pas ici qu'il faut déroger aux principes d'élaboration de la PSSI vus précédemment, car il faut bien sûr définir des règles à appliquer, mais le mode de contrôle sera différent dans le cadre de ces pratiques. En effet, on peut davantage se tourner vers du contrôle par les résultats ou par la socialisation. Ces méthodes donneront sans doute un meilleur poids à la PSSI et son application sera meilleure car bien comprise et acceptée par les utilisateurs.

2.3.5.2. Le cas de l'utilisation de l'open-source

Un autre facteur technique peut venir modifier l'orientation donnée à la PSSI. Nordine Benkeltoum a étudié l'adoption de l'open-source dans le cadre de la conception de systèmes d'information critiques et notamment chez Thalès (Benkeltoum, 2016). Thalès est une grande entreprise française pleinement investie dans la sécurisation des systèmes d'information critiques et de la donnée sensible d'entreprise. Elle travaille notamment avec les armées et les administrations françaises sur ces sujets. L'open-source est « *une méthode d'ingénierie logicielle qui consiste à développer un produit ou des composants logiciels* [tout en laissant] *en libre accès le code source produit* » (Le Mag IT, 2016).

Dans cette partie, seul l'aspect technique de l'open-source sera abordé car le choix de ce type de technologie a des impacts organisationnels qui seront décrits dans la seconde partie de ce mémoire.

La nature même du logiciel open-source fait varier de façon importante l'élaboration et la mise en œuvre d'une politique de sécurité du système d'information pour l'entreprise adoptant de tels logiciels. En effet, on l'a vu dans la définition, le code du logiciel est accessible à tous, personnes bienveillantes comme mal intentionnées. Il peut donc être techniquement facile à un attaquant d'analyser le code afin d'en déterminer les failles. Ainsi, on entrevoit déjà clairement la nécessité de mettre en place une politique permettant de satisfaire un bon niveau de sécurité du système d'information tout en utilisant des logiciels de ce type. N. Benkeltoum insiste d'ailleurs sur ces points de sécurité : « *l'application de l'open source dans des systèmes* [d'information critiques] *se heurte à d'importants freins. D'abord, du fait de l'ouverture du code source certains considèrent que le SI est davantage sujet à l'identification de failles de sécurité ou de backdoors (portes dérobées). C'est finalement l'intégration de composants inconnus qui pose le plus problème pour les professionnels de la sécurité et non le fait que le logiciel soit open source (Lawton 2002)* » (Benkeltoum, 2016).

En revanche, l'open-source peut aussi présenter des avantages non négligeables comme l'indépendance des logiciels (limitation des possibilités de recours à l'espionnage puisqu'on sait comment fonctionne le code) ou la parfaite adaptation aux pratiques et besoins de l'entreprise (comme le cas de la distribution Linux utilisée par la Gendarmerie ou des organismes étrangers tels que la NSA[3]). C'est pourquoi il peut pleinement s'inscrire dans le processus d'élaboration de la PSSI et être utilisé comme « outil de sécurité » pour le système d'information.

Quoi qu'il en soit, l'adoption ou non de tels logiciels dans un système d'information influence fortement l'élaboration et la mise en œuvre d'une politique de sécurité. Un outil utile à la décision concernant les choix à réaliser dans le cadre de l'intégration d'outils open-source dans le système d'information en matière de PSSI peut être la matrice SWOT[4]. En effet, l'analyse des forces et faiblesses ainsi que des opportunités et menaces d'un outil open-source peut conduire à faire des choix différents dans la manière de penser cette politique. Cet outil d'analyse stratégique peut d'ailleurs être utilisé quels que soient les logiciels ou matériels employés dans l'entreprise.

2.4. Conclusion

Dans cette première partie, nous avons abordé en premier lieu la définition de la politique de sécurité d'un système d'information afin de bien connaître les enjeux auxquels elle va tenter de répondre. Ensuite, dans une deuxième partie, nous avons décrit et analysé les processus d'élaboration d'une PSSI afin de réaliser un document stratégique efficace et concret pour l'entreprise. Enfin, dans un troisième temps, nous avons vu quels facteurs peuvent influencer la direction prise par l'équipe en charge de la conception de cette PSSI afin qu'elle réponde

[3] National Security Agency : agence nationale de la sécurité américaine. Cette agence est l'organisme chargé du renseignement et de la sécurité des systèmes d'information. Elle est rattachée au ministère de la Défense des États-Unis.
[4] Strengths, Weaknesses, Opportunities and Threats. Matrice présentant les forces, faiblesses ainsi que les opportunités et les menaces sur un projet ou celles d'une organisation.

réellement aux enjeux et risques définis lors de la deuxième phase de conception (phase portant sur la définition des enjeux stratégiques).

3 Impacts de la PSSI sur le mode de fonctionnement de l'entreprise

Nous allons nous concentrer sur les impacts de la politique de sécurité du système d'information sur le mode de fonctionnement de l'entreprise. Nous verrons dans un premier temps les impacts de la mise en place d'une telle politique sur l'organisation de la hiérarchie au sein de l'entreprise, notamment celle de la chaîne de commandement et du management. Nous verrons aussi que l'adoption de certaines technologies vont modifier l'organisation de l'entreprise. Dans un second temps, nous aborderons également les impacts de la PSSI sur les méthodes de management des collaborateurs, notamment pour que la politique adoptée par la direction de l'entreprise soit mise en œuvre et correctement appliquée afin qu'elle soit efficace.

3.1. Impacts sur la hiérarchisation au sein de l'entreprise

Nous allons nous intéresser aux différents impacts que peut avoir la mise en œuvre d'une politique de sécurité du système d'information sur l'entreprise, et notamment les impacts sur la hiérarchisation en place dans l'entreprise. La PSSI peut avoir en effet deux types d'impacts : un impact sur la structure de la chaîne de commandement dans l'entreprise mais aussi un impact plus structurel sur celle-ci.

3.1.1. Impacts sur la chaîne de commandement

Tout d'abord, il nous faut aborder les impacts de la PSSI sur la chaîne de commandement. On peut voir, au travers des différents articles lus dans le cadre de ce mémoire, que l'élaboration de la PSSI n'est pas sans impact sur la ou les chaînes de commandement dans l'entreprise. En effet, aussi bien Y. Barlette (Barlette, 2008; 2012) que N. Dagorn et N. Poussing (Dagorn & Poussing, 2012) décrivent des impacts organisationnels de la PSSI. Ils expliquent que suivant l'engagement de la Direction dans l'élaboration de celle-ci, des connaissances techniques qu'elle détient sur le sujet, ou de son rôle plus ou moins délégatif, la structure chargée de mener à bien ce travail sera bien différente d'une entreprise à une autre, de même que la structure résultante de ces travaux.

Si l'on prend l'exemple d'un grand groupe comme EDF, la structure de commandement concernant la sécurité du système d'information sera différente d'une entreprise ayant fait des choix structurels différents pendant les phases d'élaboration de la PSSI. EDF a choisi de créer une direction des systèmes d'information, qui a, entre autres choses, la charge de veiller au maintien des politiques existantes en matière de sécurité des systèmes d'information et à la création de nouvelles en fonction des besoins. Ainsi, ce sera la responsabilité du Directeur des Systèmes d'information du groupe EDF de veiller à remplir ces missions. Les responsables de la sécurité des systèmes d'information (RSSI) auront, par délégation du DSI, l'autorité nécessaire sur leur périmètre de sécurisation (en général une application chez EDF). Les personnes en charge de l'application de la PSSI seront donc directement pilotées par ce ou ces RSSI.

Une autre structure peut adopter une chaîne de commandement complètement différente, comme l'explique notamment Y. Barlette (Barlette, 2012). La charge de « DSI/RSSI » peut être confiée à une entreprise extérieure qui sous-traitera cette partie car elle aura davantage de compétences. Ainsi, la structure de commandement concernant l'application de la PSSI sera pilotée depuis l'extérieur de l'entreprise, tout en restant sous la responsabilité du chef d'entreprise. Une autre possibilité évoquée par Y. Barlette et constatée sur le

terrain est la délégation de la sécurité du système d'information à un salarié « volontaire », ce qui modifie encore les rapports hiérarchiques. Suivant les cas, cette hiérarchie est encore modifiée. Si ce salarié est formellement investi de cette mission, les rapports de commandement sont ainsi légitimés et plutôt bien acceptés dans l'entreprise. En revanche, Y. Barlette rapporte aussi que si ce rôle de RSSI n'est pas correctement formalisé, voire qu'il est complètement ambigu et informel, il y a alors peu de chance pour que la sécurité de la donnée d'entreprise soit correctement assurée. En effet, la mission sera seulement officieuse et des problèmes de rapports de force sont très susceptibles d'apparaître et d'être contreproductifs.

N. Dagorn et N. Poussing ont basé leur recherche sur la gouvernance de la sécurité de l'information (Dagorn & Poussing, 2012), et en effet, cette gouvernance est absolument nécessaire à la réussite de l'intégration d'une PSSI dans l'entreprise. On peut même aller jusqu'à dire que la PSSI est l'outil de choix en matière de gouvernance de la sécurité de l'information. Ainsi, l'entreprise doit bien évidemment mettre en œuvre une telle stratégie. On s'aperçoit dès lors que le terme de « gouvernance » n'est pas choisi au hasard et qu'il témoigne de l'impact de la PSSI sur la chaîne de commandement. Si l'on remet les choses dans le bon ordre, on voit bien que, chaque PSSI étant différente, chaque système de gouvernance de la sécurité de l'information sera différent. Le système de gouvernance définit l'ensemble des responsabilités qui incombent à chacun, voilà pourquoi on peut dire que la PSSI, comme outil principal de conception d'un système de gouvernance de la sécurité de l'information, modifie la chaîne de commandement en fonction de sa conception.

3.1.2. Impacts sur l'organisation structurelle de l'entreprise

On l'a bien vu, la PSSI est l'outil de prédilection pour la création d'un système efficace de gouvernance de la sécurité de la donnée. Comme toute gouvernance, celle-ci doit aussi se traduire structurellement dans l'entreprise. En effet, si des rôles sont créés, alors les personnels insérés dans ce système de gouvernance occupent des places plus ou moins définies et organisées suivant les entreprises.

Il y a une nécessité de stratifier l'organisation de celles-ci. De plus, comme on l'a vu précédemment, l'adoption de certaines technologies ou organisations du travail vient impacter la conception et la mise en place d'une politique de sécurité. Cet impact se retrouve nécessairement présent dans l'organisation du système de gouvernance dont parlent N. Dagorn et N. Poussing.

Ceux-ci précisent que selon les entreprises, la responsabilité de la gouvernance de la sécurité de la donnée peut être confiée à divers acteurs : au Directeur des Systèmes d'Information (DSI) ou à un RSSI rattaché à cette Direction, à un responsable de la qualité et de la conformité, ou encore au Directeur général. Suivant les risques encourus par l'entreprise dans ce domaine, les deux chercheurs estiment que le rattachement de cette gouvernance sera différent (Dagorn & Poussing, 2012). De même, Y. Barlette revient sur l'impact structurel de la PSSI. Il indique ainsi que le rôle de pilotage de cette politique peut être confié à différentes personnes au sein de l'entreprise comme le dirigeant (suivant son implication), un RSSI dont c'est le métier (il est en général rattaché à une DSI), un prestataire externe qui met ses compétences au service de l'entreprise ou bien encore un salarié qui prend cette mission supplémentaire (Barlette, 2012).

L'organisation structurelle de l'entreprise sera alors différente suivant le cas choisi. Si l'on prend le cas d'une PSSI sous-traitée par une entreprise extérieure, c'est sans doute le cas le plus flagrant de modification de la structure de l'entreprise car tout un pôle de compétences se trouve externalisé. Des salariés sont peut-être présents dans les locaux de l'entreprise, suivant le contrat négocié, mais ils ne lui « appartiennent » pas. En général, ce genre de sous-traitance mène à la mise en place d'une relation utilisant le télétravail pour le salarié attaché à la gestion de la PSSI de l'entreprise ayant signé ce type de contrat. Elle doit alors prendre, comme l'explique Michel Walrave, des « *mesures de sécurité technologiques et organisationnelles supplémentaires afin de protéger les données sensibles* » (Walrave, 2010). Dans ce contexte, cela influe sur la façon de communiquer à distance avec les « *collègues, les gestionnaires et les partenaires extérieurs* ». Comme on a vu que la PSSI s'intéressait également à

la problématique du télétravail, on voit bien que les choix viennent modifier la structure de l'entreprise, et ses relations avec les partenaires qu'elle peut avoir, notamment sur ces sujets.

Un autre exemple serait de prendre une équipe interne gérée par un « salarié-RSSI » (comme les appellent Y. Barlette) qui est détaché d'une partie de son activité principale pour superviser cette partie. Les impacts organisationnels sont moindres car le salarié est bien dans l'entreprise, mais il va être amené à travailler avec des collaborateurs qui ne sont pas dans la même équipe que lui. La structure des équipes est donc modifiée.

Alain Desreumaux présente quant à lui les différentes stratégies d'organisation de l'entreprise en s'appuyant notamment sur la catégorisation de Miles et Snow. Les entreprises ont souvent recourt à l'organisation selon la logique « stratégie/structure » (Desreumaux, 2015). Cela implique que c'est la stratégie de l'entreprise qui va définir sa structure. Les processus d'élaboration d'une PSSI s'inscrivent complètement dans cette logique car c'est la manière dont on va choisir d'agir qui va diriger la structure de la réponse de sécurité et de la gouvernance de la sécurité de l'information dont parlent N. Dagorn et N. Poussing. En effet, suivant la stratégie de sécurité (c'est-à-dire les choix faits en termes de périmètres surveillés par la PSSI) choisie, la gouvernance, le pilotage de la sécurité et l'organisation des équipes chargées de maintenir cette sécurité dans le système d'information surveillé vont être très fortement impactés dans leur structure.

Une autre conséquence des choix stratégiques faits en matière de sécurité du système d'information est l'organisation du service informatique de l'entreprise. M. Walrave rappelle que ce service a toute son importance dans la mise en œuvre de la PSSI car c'est souvent lui qui va être chargé de mettre en place les solutions techniques retenues, mais « *il doit également être à l'écoute des parties concernées et traduire la nécessité de la collaboration et de la communication à distance par des outils fiables et faciles d'utilisation* » (Walrave, 2010). En effet, l'écoute fait partie des missions premières de ce type de services, même si cela n'est pas souvent perçu par tous. De ce fait, l'organisation de ce service peut être

modifiée en fonction de la PSSI qui peut par exemple prévoir la création d'un pôle SSI dédié qui sera à l'écoute des besoins, qui traitera les incidents. Dans les grandes entreprises, on est généralement déjà doté de ce service, mais il a sûrement été mis en place pour répondre à un critère stratégique défini dans la PSSI. Ce service est par principe rattaché à la DSI : le SOC[5].

Prenons ici l'exemple d'EDF : chaque application dispose de sa propre PSSI. En effet, le système d'information EDF Groupe est suffisamment vaste pour qu'une stratégie de découpage soit amplement justifiée. Ainsi, chaque application (ERP[6], SIEM[7], espace client, annuaires informatiques, application cœur de CNPE[8], extranets…) est régie par une PSSI. Chaque application est donc surveillée différemment, en fonction des risques qui lui sont propres. Un RSSI, rattaché à la DSI Groupe, est responsable de la surveillance d'un périmètre (d'une application) en particulier. Ce RSSI va travailler avec les agents concernés par l'application ainsi que les agents du SOC qui surveillent l'ensemble de la sécurité du système d'information d'EDF. L'organisation de cette structure permet donc bien de voir que celle-ci est effectivement dirigée par les choix stratégiques faits lors de l'élaboration de la PSSI.

Les conclusions de N. Benkeltoum semblent également indiquer que l'adoption de logiciels ou de briques open-source a un impact sur l'organisation structurelle de l'entreprise. En effet, dans le cadre son étude sur Thalès (Benkeltoum, 2016), il dit que Capra *et al.* ont mené une recherche sur les avantages et les inconvénients structurels de l'open-source en 2011.

De plus, il indique que l'adoption stratégique de technologies open-source (et cela peut rentrer dans le cadre de la PSSI, on l'a vu) a plusieurs impacts organisationnels. Il cite en particulier le fait que l'utilisation de ce type de logiciels conduit au « *déploiement de « forges internes » ou au développement de compétences spécifiques* » (Benkeltoum, 2016). C'est ce qu'a d'ailleurs fait le

[5] Security Operation Center, centre opérationnel de sécurité.
[6] Enterprise Ressource Planning, ou Progiciel de Gestion Intégré (PGI).
[7] Security Information and Event Management, système de gestion de l'information et des événements de sécurité.
[8] Centrale Nucléaire de Production d'Électricité.

groupe Thalès, et bien pour des raisons de sécurité des solutions qu'il peut proposer sur le marché. En effet, l'utilisation de tels logiciels peut conduire à la création de nouvelles équipes chargées du maintien de ces technologies, de la conception de nouvelles briques open-source en fonction des besoins spécifiques rencontrés ou nécessaires pour adapter l'outil au cas d'usage concret de l'entreprise (ce qui est d'ailleurs l'intérêt des logiciels open-source) ou de veille concernant les potentielles vulnérabilités de sécurité.

Comme le dit aussi N. Benkeltoum, l'adoption d'outils open-source conduit aussi parfois à développer de nouvelles compétences spécifiques, ou bien à les attirer dans l'entreprise par le biais de recrutement. Ainsi, on modifie la structure organisationnelle car il va sans doute falloir agrandir les équipes (ce qui peut, en fonction des règles de management, conduire à la création de nouvelles équipes) ou bien en créer de nouvelles spécifiques à de nouvelles compétences. N. Benkeltoum cite finalement un interrogé lors de son enquête dans le cadre de sa recherche : cette personne confie que l'« *open-source a un pouvoir inné de transformer les organisations même les plus fermées et les plus policées* » (Benkeltoum, 2016). L'open-source a donc un réel impact structurel sur l'entreprise.

3.2. Impacts sur le management dans l'entreprise

Après avoir abordé les impacts organisationnels et structurels sur l'entreprise, nous allons nous attarder sur les impacts que la PSSI engendre sur le management dans l'entreprise. La PSSI est un document qui met en place des règles afin de répondre à une stratégie particulière de sécurité de la donnée, comme on l'a déjà vu. Ces règles sont bien sûr directrices pour les actions techniques à mettre en place au niveau même du système d'information, ou en tout cas du périmètre surveillé par la PSSI, mais elle contient également tout un ensemble de règles plus « comportementales » qui viennent s'appliquer à chaque utilisateur du système d'information.

Nous allons donc d'abord voir quels sont les impacts concrets en termes de management des collaborateurs, puis ensuite l'apport que le management peut

constituer pour la sécurité du système d'information. En effet, le management peut être un facteur influenceur de la sécurité du système d'information, nous étudierons pourquoi.

3.2.1. PSSI et management des collaborateurs

La PSSI a un impact direct sur le management des collaborateurs, notamment dans les départements informatiques qui sont particulièrement sensibles à ce niveau. En effet, les collaborateurs sont, tout comme la technologie, en première ligne pour la sécurité du système d'information. L'argument principal venant appuyer cette idée est bien entendu le fait que l'entreprise peut se doter des meilleurs équipements techniques, avoir les meilleures règles de contrôle d'accès sur ses pares-feux ou autres, si l'humain commet une erreur, alors la sécurité du système d'information sera compromise, malgré toutes les mesures techniques mises en œuvre.

3.2.1.1. Problèmes que peut rencontrer le management

On voit bien alors qu'il faut intégrer le facteur humain dans la PSSI et c'est ce qui a normalement été fait lors de son élaboration et de son déploiement à l'échelle de l'entreprise. On peut notamment faire référence aux chartes informatiques que tout le monde a déjà signé lors de son arrivée en entreprise. Ces chartes font partie intégrante du management des collaborateurs en matière de sécurité du système d'information.

É. Thenoz aborde dans son article la gestion des usages des technologies numériques notamment par le contrôle organisationnel et le biais des chartes informatiques (Thenoz, 2020). Il explique bien que l'usage de telles technologies engendre des points de frictions entre l'utilisateur et l'entreprise. En effet, tous deux n'ont pas forcément la même vision de l'usage du matériel informatique et d'Internet, notamment à cause de « *la continuité entre usages domestiques et professionnelles de* [ces] *technologies* » (ibid.). Cette tension peut se manifester notamment par l'usage du Shadow IT, phénomène difficilement contrôlable et bien souvent problématique pour la sécurité. Le Shadow IT est le terme désignant

l'usage d'outils, de techniques, de technologies ou plus généralement de pratiques non autorisés dans la politique de sécurité de l'entreprise afin de contourner des restrictions qui nuisent, selon les utilisateurs les mettant en place, à leur productivité au travail.

Le management peut aussi être confronté à des utilisateurs qui ne veulent pas respecter les principes car ils ne les comprennent pas forcément bien, ni d'ailleurs les raisons pour lesquelles ils ont été mis en œuvre dans l'entreprise, ou encore à ceux qui n'ont pas conscience des risques que certaines pratiques font courir au système d'information et à l'entreprise plus globalement. Dans certaines entreprises, les employés recourent à l'usage des réseaux sociaux pendant le temps de travail (et bien sûr en dehors) et parfois depuis leur poste professionnel. Ces pratiques peuvent conduire à la fuite d'informations vers l'extérieur, sachant qu'on le sait pertinemment aujourd'hui, les réseaux sociaux sont très friands des données personnelles de leurs utilisateurs.

Dans le même registre, on peut aussi constater le recours à des solutions de cloud grand public pour stocker de la donnée d'entreprise pour peut-être pouvoir travailler à domicile sur certains sujets, ou bien alors sauvegarder un travail important. Le problème principal est que, en général, travail important signifie souvent travail stratégique pour l'entreprise. Un travail stratégique est d'ailleurs souvent confidentiel ou à diffusion restreinte. Ainsi, le mettre sur un cloud public type OneDrive ou Google n'est souvent pas permis par les entreprises, car ces données échappent à son contrôle et tombent rapidement dans les mains des prestataires, encore une fois très gourmands en données personnelles, que peuvent être Microsoft ou Google, dans les exemples cités ici.

Pour prendre un exemple concret, on peut clairement lire dans la charte informatique d'EDF une clause concernant le stockage des données professionnelles. Il y est clairement stipulé que « *l'utilisation de supports de données non avalisés par l'entreprise à des fins de stockage des documents professionnels est formellement interdite* » (charte informatique du Groupe EDF). Dans la liste des supports non avalisés donnés par EDF, on compte bien sûr les solutions de cloud personnel, parmi lesquelles les exemples cités plus avant.

Ainsi, on voit bien la réalité de ce genre de comportements et de clauses. De plus, même au sein de l'entreprise, il existe une classification des moyens de stockage pour la donnée en fonction de sa confidentialité. Par exemple, il est demandé aux salariés de ne pas stocker des informations classées en C3 (confidentiel) sur les serveurs OneDrive alors même qu'ils sont souscrits par l'entreprise. En effet, ils ne sont pas jugés suffisamment sûrs pour l'hébergement de telles données.

On a aussi vu précédemment que l'utilisation du BYOD en entreprise pouvait avoir un impact sur les principes de sécurité déclinés dans la PSSI. Cet usage demande beaucoup de contrôle de la part de l'entreprise, et il est souvent bien difficile d'y parvenir étant donné que le recours au Shadow IT est possiblement (et souvent) multiplié car le poste de l'utilisateur est sa propriété, et non celle de l'entreprise. C'est pourquoi l'application de la PSSI va fortement challenger le management qui va devoir mettre en place des méthodes afin de pouvoir garantir au mieux la sécurité des pratiques des collaborateurs.

Une fois cet état des lieux des défis à relever par le corps managérial de l'entreprise dressé, il faut trouver des solutions pour répondre à ces enjeux et garantir la sécurité du système d'information en garantissant le respect des principes énoncés dans la PSSI.

3.2.1.2. Solutions de contrôle envisageables

Dans son étude, É. Thenoz s'appuie sur les modes de contrôles développés par Ouchi en 1979 pour répondre à ces problématiques de contrôle par le management de l'application des chartes informatiques. Ces chartes étant en réalité une partie de la déclinaison concrète de la PSSI dans l'entreprise, nous pouvons ainsi utiliser les résultats qu'il présente afin de traiter notre problématique.

Les trois modes de contrôle qu'il présente sont le contrôle par le comportement, par les résultats ou bien par sociabilisation. Dans la première forme, on évalue majoritairement la conformité des comportements des utilisateurs face à des

règles. Les chartes informatiques dont parle É. Thenoz sont en grande majorité le reflet des règles mises en place dans la PSSI. Ainsi, il faut s'assurer que ces règles sont comprises et appliquées. Le contrôle par le comportement essaie donc de mettre en adéquation le comportement de l'utilisateur pour le plaquer sur la règle et faire qu'il corresponde. En cas d'écart de comportement, la règle n'est plus considérée comme respectée. Le management s'appuie alors notamment sur la surveillance informatique de ces comportements.

Cette surveillance peut être réalisée par des mécanismes mettant en jeu de l'intelligence artificielle ou au moins un algorithme de prédiction des comportements dans les plus grosses structures (qui ont donc un nombre élevé de salariés à « contrôler »). Le principe de ces algorithmes est d'analyser les comportements des utilisateurs vis-à-vis de règles et d'anticiper les attitudes déviantes compromettantes pour la sécurité du système d'information suffisamment tôt afin de les éviter. Cela est un outil qui permet d'aider le management à effectuer le contrôle par le comportement et d'y remédier en ayant par exemple un entretien avec le salarié pour comprendre pourquoi il a pu avoir ces agissements problématiques et résoudre les problèmes en mettant en place les solutions nécessaires.

En effet, on a pu le voir auparavant quand on a abordé le Shadow IT, mais certains comportements sont issus d'un blocage qui empêche, selon la personne, la réalisation correcte du travail. Ainsi, avoir un entretien avec le manager et par exemple un responsable technique peut permettre de remédier à la cause principale qui conduit à ce comportement néfaste pour la sécurité du système d'information. D'autres solutions peuvent exister, mais il très compliqué de citer des exemples théoriques sachant que chaque manager a sa propre méthode de management pour redresser les comportements mettant en péril cette sécurité.

Ensuite, le management peut aussi avoir recours, comme l'explique É. Thenoz, au contrôle par les résultats. Ici, on va plutôt s'intéresser à la mesure et à l'évaluation des résultats de l'usage plutôt que celle de conformité des comportements vis-à-vis de règles. Les indicateurs sont donc complètement différents. Ainsi, le management va être plus sensible à la mesure des variables

en cherchant à responsabiliser l'utilisateur sur les résultats plutôt que sur les moyens de les atteindre. On va donc jouer sur la responsabilisation de l'utilisateur en lui mettant en lumière les conséquences concrètes qu'ont ses actes sur la sécurité du système d'information. Par exemple, cela peut être dans le cas de l'utilisation d'une clé USB pour stocker des documents confidentiels. Le management pourra ainsi détailler les impacts que cette pratique peut avoir pour l'entreprise. En cas de vol ou de perte de cette clé USB, l'utilisateur sera responsable de la fuite d'informations stratégiques capitales pour l'entreprise si le support ou les documents n'ont pas été chiffrés par exemple.

Un autre exemple plus méconnu peut être l'utilisation d'une clé USB « trouvée ». Chez EDF (et au sein des filiales), des campagnes dites « de clés USB » sont régulièrement organisées par le SOC Groupe pour sensibiliser les personnels aux risques que cela représente. Une clé USB « trouvée » peut contenir des logiciels hautement malveillants, qui peuvent même conduire jusqu'à la destruction du matériel sur lequel ils sont connectés. On voit bien l'importance que cela peut avoir sur un système d'information. Le management peut, dans le cadre du contrôle par les résultats, montrer à l'utilisateur que son acte a d'énormes conséquences sur la sécurité du système d'information.

Ce contrôle peut être renforcé et/ou remplacé par le contrôle par la sociabilisation, la dernière forme de contrôle établie par Ouchi et décrit par É. Thenoz. Le management aura ici à cœur de réaliser l'internalisation des normes et des valeurs de l'organisation par les utilisateurs. Il s'agira ici de favoriser l'intégration des bons comportements par les utilisateurs en les formant et en leur inculquant les bonnes pratiques. Ces bonnes pratiques devront être expliquées, du début à la fin, pour faire comprendre aux collaborateurs les tenants et aboutissants des règles déclinées dans la PSSI afin que, une fois celles-ci bien comprises, elles puissent être appliquées de plein gré et non plus sous la contrainte d'une menace ou d'une sanction, comme on peut le trouver dans une méthode de management basée sur le contrôle par les comportements.

Dans cette situation de contrôle, le management sera donc beaucoup plus orienté sur la sensibilisation, la favorisation d'ateliers qui permettent la diffusion

des bonnes pratiques entre collègues, en privilégiant l'esprit d'équipe et la collaboration, le « *mentorat informel ou le développement d'un climat de confiance dans et avec les équipes* » (Thenoz, 2020). On se focalisera donc beaucoup plus sur la création d'un climat qui permette d'inciter les collaborateurs au respect consenti des règles et la transmission entre pairs. É. Thenoz parle aussi de favoriser « *l'autocontrôle et la motivation intrinsèque* » des équipiers (ibid.).

Dans le contexte de la PSSI du groupe EDF, une grande attention est portée sur ce contrôle par la sociabilisation par la délivrance de nombreuses formations et campagnes de sensibilisation sur mesure créées par le SOC. Les différentes directions du groupe demandent régulièrement une campagne de sensibilisation au *phishing*, des campagnes de clés USB comme évoqué plus avant, des formations sur les dangers plus spécifiques au contexte métier. Les équipes du SOC mettent un point d'honneur à rendre leurs interventions le plus abordable possible afin de favoriser les bons comportements par la sociabilisation. On voit bien dans l'exemple du groupe EDF que c'est le management qui est à l'initiative de la demande puisque c'est le directeur (par exemple le directeur de la Direction « Commerce ») qui formule la demande au SOC pour la mise en place d'une campagne de clés USB dans ses locaux.

Si l'on doit bien retenir quelque chose de l'importance du management dans le respect de la PSSI, c'est É. Thenoz qui le formule très bien : « *nous proposons donc qu'un système de contrôle des usages des technologies numériques doive simultanément répondre à ces demandes paradoxales pour exploiter les technologies numériques efficacement en maîtrisant les tensions issues de leur usage* » (Thenoz, 2020). Le contrôle doit donc répondre aux attentes des utilisateurs de façon assez flexible pour ne pas être trop rigide et donc accentuer les déviances vis-à-vis de la PSSI établie, mais aussi faire respecter les exigences de sécurité qui ne peuvent pas être adaptées dans le résultat. On s'attachera donc, pour le management, à possiblement adapter les façons d'atteindre ces résultats. En tout cas, on voit bien que la PSSI a un impact sur le management des collaborateurs.

3.2.2. Nécessité du management pour assurer la sécurité du système d'information

On s'attachera ici à la démonstration de la nécessité du management pour garantir une sécurité suffisante du système d'information. En effet, et il faut insister sur ce point, on aura pu tout mettre en œuvre pour avoir le meilleur système de protection pour sécuriser le système d'information (on entend par là la sécurisation aussi bien technologique que physique), le facteur humain restera tout de même le maillon faible de la boucle.

La PSSI peut s'appuyer sur des éléments très bien conçus tels que la gestion des mots de passe, la configuration des équipements et des règles qui, pour être déjouées, doivent être contournées de façon extrêmement difficile (cela réduisant par conséquent la surface d'attaque et donc la probabilité d'une compromission de la sécurité du système d'information). En revanche, si l'humain, qui rappelons-le, est au cœur de ce système, défaille (ce qui n'est malheureusement pas impossible), alors la construction s'écroule, comme pourrait le faire un château de cartes auquel on retirerait la moindre carte le composant.

Le collaborateur définit ses mots de passe qui sont, la plupart du temps, régis par une politique définie dans la PSSI. Ce collaborateur, par peur d'oublier un mot de passe possiblement long ou fréquemment modifié, peut par exemple l'écrire sur un post-it ou bien l'inscrire dans un cahier ou un classeur Excel. En revanche, un tiers peut très bien récupérer ce post-it, lire cette page de cahier ou bien entrer en possession de ce fichier Excel. Il sera alors en possession d'un secret qui lui permettra de réaliser des opérations malintentionnées sur le réseau de l'entreprise. Pourtant, le collaborateur n'a pas enfreint la politique des mots de passe.

Le management devra être attentif à tous ces comportements qui mettent en danger la sécurité du système d'information malgré le fait que les consignes établies par la PSSI sont respectées. Ils sont aussi les personnes privilégiées pour faire remonter des observations du terrain qui peuvent grandement améliorer la PSSI. Dans cet exemple, le manager ayant été témoin de ce genre

de pratiques pourrait les faire remonter à l'équipe projet et ainsi conduire à la mise en place de l'utilisation obligatoire d'un gestionnaire de mots de passe sécurisé (à condition bien sûr de ne pas tomber dans le même travers en notant le mot de passe maître de ce gestionnaire sur une feuille volante ou un post-it).

Un autre élément qui mérite d'être ici souligné est l'importance du management dans la détection des éléments sensibles ou fragiles de leur équipe. En effet, un collaborateur fragile, par exemple en début de risque psychosociaux (RPS) peut conduire à une faille dans la sécurité du système d'information. Un autre exemple de collaborateur que l'on peut qualifier de sensible serait un collaborateur important au sein de l'organisation et qui est régulièrement démarché par des concurrents.

Ces collaborateurs peuvent, aussi bien pour l'une ou pour l'autre de ces catégories, représenter un risque pour l'atteinte des objectifs de sécurisation du système d'information. En effet, le premier peut, du fait de sa fragilité, conduire à divulguer à des tiers des informations sensibles qu'il devrait normalement garder pour lui, ou bien être beaucoup plus distrait et donc moins vigilant car préoccupé ou stressé et là encore divulguer des informations sensibles comme des identifiants ou autres. Pour le second exemple abordé plus avant, les collaborateurs souvent démarchés par les concurrents peuvent se révéler être des sources de renseignements en faisant fuiter volontairement des informations contre une gratification avantageuse, ou en sabotant.

Le management est donc en première ligne pour détecter rapidement ces éléments pouvant venir compromettre la sécurité du système d'information. En effet, celui-ci est au plus proche du terrain car il peut suivre les collaborateurs et agir rapidement par des entretiens ou une attention plus grande portée à ces cibles faciles pour attaquants et/ou concurrents.

3.3. Conclusion

Dans cette seconde partie, nous avons pu voir dans un premier temps les impacts qu'a la PSSI sur l'organisation hiérarchique au sein de l'entreprise en

évoquant particulièrement les enjeux qu'elle fait porter sur la chaîne de commandement et de décision ainsi que son impact plus structurel. Cela nous aura donc permis d'étudier les conséquences des choix stratégiques faits lors des phases nécessaires à l'élaboration de la PSSI.

Ces choix se répercutent également sur le management dans l'entreprise. Nous avons pu voir concrètement comment la PSSI influe directement sur les méthodes de management et les enjeux que cela représente. Nous avons pu aussi nous rendre compte que le management est un maillon essentiel dans la sécurité du système d'information car l'humain est malheureusement le point faible dans un certain nombre de situation. Ainsi, il appartient au management de détecter les comportements et collaborateurs « à risques » pour la sécurité du système d'information.

4 Conclusion

Dans ce mémoire, nous avons attaché beaucoup d'importance à décrire la politique de sécurité du système d'information en définissant assez précisément le sens qu'a cette politique puis en donnant les grandes étapes clés nécessaires à l'élaboration d'une bonne politique de sécurité. Nous avons également décrit les différents facteurs qui sont susceptibles de modifier les orientations stratégiques de la PSSI afin de comprendre aussi ce qui la modèle et ce qui doit être pris en compte lors de son élaboration. Dans un second temps, nous avons pris le temps d'observer quels impacts peut avoir le développement d'une telle politique dans l'entreprise, non seulement en termes organisationnels et hiérarchiques, mais également en termes managériaux. On a ainsi pu se rendre bien compte de tout ce qu'impliquait comme changements la mise en place d'une démarche de gouvernance de la sécurité de la donnée.

Le questionnement auquel nous devions répondre était : « *Pourquoi la politique de sécurité du système d'information d'une organisation impacte-t-elle directement son mode de fonctionnement ?* ». Après avoir vu tous les éléments résumés plus haut, nous pouvons clairement dire que la PSSI d'une entreprise impacte son fonctionnement parce que c'est un document définissant une stratégie particulière de gouvernance de la sécurité de la donnée.

Comme tout document stratégique, il doit être décliné verticalement à tous les niveaux de l'entreprise et a de ce fait un impact non négligeable sur le mode de fonctionnement de l'entreprise. En effet, son but est de construire une réponse adaptée aux risques encourus et de modifier les comportements. On parle en fait d'amélioration de « l'hygiène informatique »[9] des utilisateurs. Toutes les

[9] C'est effectivement le terme employé dans les métiers de la cybersécurité, même s'il peut paraître surprenant.

directives prises dans la PSSI doivent l'être dans l'intérêt de la sécurité du système d'information de l'entreprise. Ces changements vont donc nécessiter des adaptations dans le fonctionnement de l'entreprise, aussi bien en termes d'organisation que de management. Par exemple, la PSSI peut vouloir décider la création d'une équipe SOC si l'entreprise n'en bénéficiait pas déjà, ou alors décider d'instaurer l'une au l'autre des méthodes de management vues dans les points précédents.

De notre point de vue, la PSSI est aujourd'hui un document essentiel à toute entreprise car tout est informatisé, ou en passe de l'être. L'expérience montre que si le système d'information d'une entité, quelle qu'elle soit, vient à tomber (suite à une panne ou à une faille de sécurité), tout devient compliqué. Un exemple très simple peut venir appuyer ce propos. On a pu voir en mars 2021 l'impact qu'a pu avoir l'incendie du site de Strasbourg de l'hébergeur français OVH sur les entreprises européennes. Il faut imaginer les mêmes conséquences en cas d'attaques informatiques.

En effet, les données des petites et moyennes entreprises sont rarement stockées sur un système d'information interne à l'entreprise du fait de leur taille et de leurs moyens limités. Ainsi, elles délèguent souvent la gestion de la donnée à une entreprise telle qu'OVH. Si des personnes malintentionnées utilisent les postes des employés pour accéder au système d'information « on cloud »[10], alors toute la donnée sera perdue. C'est la même situation pour les systèmes d'information « on premise » dans le cas des plus grosses structures.

De manière générale, dans le cadre des PME, on délègue seulement une partie de la PSSI à l'hébergeur qui doit, de son côté, sécuriser ses infrastructures proposées à la location, par la redondance des serveurs de sauvegarde sur un second site distant par exemple. En revanche, une partie de la PSSI reste à la charge de l'entreprise, car si l'hébergeur fournit les infrastructures, c'est bien à l'entreprise de sécuriser la manière de les exploiter. On voit donc bien que, dans

[10] Par opposition au système d'information « on premise », c'est-à-dire sur site ou propriété de l'entreprise.

tous les cas de figure, l'entreprise ne peut pas se dédouaner de l'engagement qu'elle doit prendre en termes d'élaboration de sa propre PSSI. Ainsi, celle-ci a toujours un impact sur l'entreprise.

Lors des recherches documentaires, on a été confronté au manque de publications sur le sujet de la PSSI et de ses impacts organisationnels. Pourtant, ce sujet semble riche en possibilités d'exploration. Ainsi, une perspective de recherche serait de s'ouvrir à cette vaste thématique qui, à l'heure actuelle, n'est peut-être pas suffisamment explorée. On pourrait proposer de nombreux sujets de recherche dans ce domaine. L'informatique, de manière générale, se développe à grande vitesse dans les entreprises et cela implique de nombreux impacts. Les sciences de gestion pourraient se saisir de certaines de ces thématiques intéressantes à étudier.

Plusieurs exemples peuvent être envisagés. On pourrait étudier l'impact du télétravail sur les méthodes de management, sur les procédures de recrutement ou de gestion des ressources humaines. L'étude de certains sujets comme les impacts relationnels de l'utilisation massive de l'informatique dans les entreprises (un exemple simple serait le choix d'envoyer des mails à ses collègues dans le même bureau alors qu'il serait plus simple de discuter avec eux) ouvre également des perspectives de recherche intéressantes, larges et pour l'heure peu abordées.

Une autre piste serait d'explorer les évolutions qu'ont dû entreprendre les entreprises durant la crise sanitaire du Covid-19, notamment les évolutions informatiques au niveau de la PSSI. En effet, le télétravail massif a bouleversé les pratiques et les organisations. On peut dire qu'il y a une ère « pré-Covid » et une ère « post-Covid » dans ce domaine. Il paraît intéressant de mener des recherches dans ce sens, et c'est un regret de ne pas avoir eu assez de recul pour en parler dans ce mémoire car il aurait été très intéressant de le faire, étant donné que les impacts des PSSI ont vraiment été exacerbés pendant cette période.

À travers ce mémoire, j'ai pu mieux appréhender l'importance des sciences de gestion au quotidien car elles permettent de faire des liens entre la technique et l'organisationnel. Ce lien est extrêmement important pour la compréhension et l'adhésion à toute politique d'entreprise dont la PSSI fait partie, et qui a été notre fil conducteur. Ainsi, cela permet de mieux comprendre les interactions entre les décisions stratégiques qui sont prises et on a pu mieux voir les impacts résultants de telles décisions.

Bibliographie

Agence Nationale de la Sécurité des Systèmes d'Information. (2004). *Guide d'élaboration de Politiques de Sécurité des Systèmes d'Information.* DCSSI. Paris: Premier Ministre, SGDN.

Alric, J.-Y. (2021, mars 17). *Ransomwares : le montant moyen des rançons est en forte augmentation.* Consulté le juin 27, 2021, sur Presse Citron: https://www.presse-citron.net/ransomwares-le-montant-moyen-des-rancons-est-en-forte-augmentation/

Barlette, Y. (2008). Une étude des comportements liés à la sécurité des systèmes d'information en PME. *Systèmes d'information et management, Volume 13*, pp. 7-30. Récupéré sur https://www-cairn-info.proxy-bu1.u-bourgogne.fr/revue-systemes-d-information-et-management-2008-4-page-7.htm

Barlette, Y. (2012). Implication et action des dirigeants : quelles pistes pour améliorer la sécurité de l'information en PME ? *Systèmes d'information et management, Volume 17*, pp. 115-149. Récupéré sur https://www-cairn-info.proxy-bu1.u-bourgogne.fr/revue-systemes-d-information-et-management-2012-2-page-115.htm

Benkeltoum, N. (2016). Adoption de l'open source pour la conception de systèmes d'information critiques : le cas Thales. *Systèmes d'information et management*, pp. 71-98. Récupéré sur https://www-cairn-info.proxy-bu1.u-bourgogne.fr/revue-systemes-d-information-et-management-2016-4-page-71.htm

Dagorn, N., & Poussing, N. (2012). Engagement et pratiques des organisations en matière de gouvernance de la sécurité de l'information. *Systèmes*

d'information et management, Volume 17, pp. 113-143. Récupéré sur https://www-cairn-info.proxy-bu1.u-bourgogne.fr/revue-systemes-d-information-et-management-2012-1-page-113.htm

Desreumaux, A. (2015). Nouvelles formes d'organisation et évolution de l'entreprise. *Revue française de gestion*, pp. 139-172. Récupéré sur https://www-cairn-info.proxy-bu1.u-bourgogne.fr/revue-francaise-de-gestion-2015-8-page-139.htm

Johnston, A., & Hale, R. (2009). Improved Security through Information Security Governance. *Communications of the ACM, Volume 52*, pp. 126-129. Récupéré sur https://doi-org.proxy-bu1.u-bourgogne.fr/10.1145/1435417.1435446

Le Mag IT. (2016, août). *Définition : open source.* Consulté le juillet 11, 2021, sur Le Mag IT: https://www.lemagit.fr/definition/Open-Source

Mignerat, M., Mirabeau, L., & Proulx, K. (2019). Comportements stratégiques autonomes et pressions institutionnelles : le cas du BYOD. *Systèmes d'information et management*, pp. 7-46. Récupéré sur https://www-cairn-info.proxy-bu1.u-bourgogne.fr/revue-systemes-d-information-et-management-2019-2-page-7.htm

Pereira, B. (2018). Mutation du rapport de subordination : le salarié « autonome » ou l'indépendant « subordonné » en France. *Management & Avenir*(N°104), pp. 37-56. Récupéré sur https://www-cairn-info.proxy-bu1.u-bourgogne.fr/revue-management-et-avenir-2018-6-page-37.htm

Sophos. (2021, avril 27). *Le coût lié à la reprise d'activité après une attaque par ransomware a plus que doublé par rapport à l'année dernière, atteignant désormais près de 1,6 million d'euros, selon une étude Sophos.* Consulté le juin 27, 2021, sur Sophos: https://www.sophos.com/fr-fr/press-office/press-releases/2021/04/ransomware-recovery-cost-reaches-nearly-dollar-2-million-more-than-doubling-in-a-year.aspx

Thenoz, É. (2020). Gestion des usages des technologies numériques dans les organisations : une approche qualitative par le contrôle organisationnel et les chartes informatiques. *Systèmes d'information et managament*, pp. 51-86. Récupéré sur https://www-cairn-info.proxy-bu1.u-bourgogne.fr/revue-systemes-d-information-et-management-2020-3-page-51.htm

Walrave, M. (2010). Comment introduire le télétravail ? *Gestion*, pp. 76-87. Récupéré sur https://www-cairn-info.proxy-bu1.u-bourgogne.fr/revue-gestion-2010-1-page-76.htm

Résumé – La sécurité du système d'information est aujourd'hui un enjeu grandissant pour les entreprises. En effet, elles sont tout d'abord de plus en plus dépendantes du numérique. De plus, l'augmentation des attaques cyber et les coûts engendrés en cas de succès de celles-ci sont de plus en plus importants. Les entreprises se doivent donc de se défendre et d'être protégées contre de telles menaces. De nombreuses mesures de protection techniques existent mais elles doivent être coordonnées et répertoriées. La technique n'est pas la seule composante dans l'élaboration d'une stratégie de sécurité de la donnée : le facteur humain entre également en jeu. C'est pourquoi les entreprises élaborent des politiques de sécurité pour leurs systèmes d'information. Ce mémoire étudiera l'impact de telles politiques sur l'organisation des entreprises.

Mots-clés : politique de sécurité, impact, fonctionnement, entreprise, management

Abstract – The security of the information systems is nowadays a huge and increasing concern for companies. They are indeed more and more reliant on digital technologies. Furthermore, the number of cyberattacks and their cost are always increasing, month after month. That is why companies have to be more protected and should fight against these threats. A lot of technical procedures can be implemented but they must be classified and coordinated. But technics is not the only component of the cyber-response: the human factor is also important. That is why companies formulate some security policies for their information systems. This dissertation will review the impact that these policies have on the enterprise structure.

Keywords : security policy, impact, operating, corporation, management