h e g

Sensibilisation à la sécurité du système d'information : Moyens utilisés, impacts observés, comment améliorer ?

Travail de Bachelor réalisé en vue de l'obtention du Bachelor HES

par :

Claire-Stefanie BORBOËN

Conseiller au travail de Bachelor :

Rolf HAURI, Chargé d'enseignement HES

Carouge, le 30 septembre 2013

Haute École de Gestion de Genève (HEG-GE)

Filière Informatique de Gestion

Hes·so GENÈVE
Haute Ecole Spécialisée de Suisse occidentale

Déclaration

Ce travail de Bachelor est réalisé dans le cadre de l'examen final de la Haute école de gestion de Genève, en vue de l'obtention du titre de Bachelor en Informatique de Gestion. L'étudiant accepte, le cas échéant, la clause de confidentialité. L'utilisation des conclusions et recommandations formulées dans le travail de Bachelor, sans préjuger de leur valeur, n'engage ni la responsabilité de l'auteur, ni celle du conseiller au travail de Bachelor, du juré et de la HEG.

« J'atteste avoir réalisé seule le présent travail, sans avoir utilisé des sources autres que celles citées dans la bibliographie. »

Fait à Carouge, le 30 septembre 2013

Claire-Stefanie Borboën

Remerciements

Tout d'abord, je tiens à remercier Monsieur Rolf HAURI qui m'a suivi tout au long de ce travail et s'est toujours montré disponible pour répondre à mes questions. Ses conseils et ses relectures m'ont permis d'aiguiller mes recherches.

Je remercie également les trois professionnels des entreprises privées, et tous les collaborateurs de la Haute Ecole de Gestion et de la Haute Ecole de Santé de Genève qui ont pris du temps pour répondre à mes interviews. Leurs précieuses réponses m'ont permis d'aboutir à ce présent travail.

Enfin, je tiens aussi à remercier mes parents pour leur soutien, leurs relectures attentives et leurs suggestions de lecture.

Résumé

Une entreprise doit pouvoir assurer la valeur de ses informations, comme ses informations commerciales, clients, fournisseurs ou sous-traitants, ou encore ses secrets de fabrication. Elle doit aussi protéger son patrimoine ou encore son savoir-faire, afin de rester compétitive sur le marché économique et préserver sa réputation.

Pour pallier aux différents types de menaces qui pèsent sur son système d'information, une entreprise doit mettre en place un ensemble de moyens techniques, organisationnels, juridiques et humains, pour protéger ses ressources et garantir ses activités.

Dans ce travail, nous nous sommes concentrés spécifiquement sur les mesures humaines, qui visent à informer, former et sensibiliser les employés de l'entreprise.

Pour répondre à cette problématique, nous avons dans un premier temps cerné le rôle et les enjeux de la sécurité du système d'information, afin de comprendre dans quel contexte la sensibilisation doit s'effectuer.

Nous avons ensuite analysé les raisons pour lesquelles il est important de sensibiliser les employés. Les méthodes recommandées par les organismes mondialement reconnus pour mener à bien une campagne de sensibilisation, sont aussi couvertes dans ce document.

Pour finir, nous avons proposé une approche pour améliorer la sensibilisation au sein des deux Hautes Ecoles Spécialisées de Genève, pour réduire le facteur de risque humain qui pèse sur son système d'information.

Table des matières

Déclaration i
Remerciements ii
Résumé iii
Table des matières iv
Liste des tableaux vii
Liste des figures vii
1. Introduction 1
1.1 Problématique 1
1.2 Méthodologie de travail 1
2. Rôle et enjeux du système d'information 3
2.1 L'information 3
2.2 Le système d'information 3
2.2.1 Types de menaces 4
2.2.2 Conséquences 5
2.3 La sécurité du système d'information 5
2.3.1 Principes fondamentaux de la sécurité 5
2.3.2 Responsable de la sécurité du système d'information 6
2.3.3 Types de mesures de sécurité 7
3. Le facteur risque humain 9
3.1 Définition 9
3.2 L'importance de ce risque 10
3.3 Les vecteurs de menaces 12
4. La sensibilisation 15
4.1 Définition 15
4.2 Dimensions 16
4.3 Pour quelles raisons sensibiliser 18
4.3.1 Peu conscients de l'importance de la sécurité 18
4.3.2 Nouvelle génération, nouveaux risques 19
4.4 Intégrer la sensibilisation dans le processus de sécurité 21
4.5 Statistiques actuelles en entreprise 23
4.5.1 Baisse des programmes de sensibilisation 23
4.5.2 Personnel dédié 24
4.5.3 Budget 24
4.6 Conclusion 25
5. Processus de sensibilisation 26
5.1 Norme 26

5.1.1 Norme ISO 27002....26
5.2 Méthodes....30
5.2.1 Planification....32
5.2.2 Conception....33
5.2.3 Diffusion....34
5.2.4 Evaluation....34
5.2.5 Maintenance....35
5.3 Comment adapter la communication....36
5.3.1 Convaincre, communiquer et impliquer....36
5.3.2 Message court et original....36
5.3.3 Moyen interactif....37
5.3.4 Tester les connaissances....37
5.4 Les canaux de communication....38
5.5 Solution informatique....39
5.6 Conclusion....39
6. Dans la réalité....40
6.1 Interviews - secteur privé....40
6.1.1 Banque....40
6.1.2 Multinationale....42
6.1.3 PME....45
6.1.4 Impacts de la sensibilisation dans le secteur privé....47
6.2 Interviews - Hautes Ecoles Spécialisées....48
6.2.1 Haute Ecole de Santé....48
6.2.2 Haute Ecole de Gestion....51
6.2.3 Impacts de la sensibilisation en HES....53
6.2.4 Conclusion....54
7. Mise en place dans un cas concret....55
7.1 Planification de la sensibilisation....56
7.1.1 Acteurs impliqués....56
7.1.2 Organisation....57
7.1.3 Evaluation du budget à obtenir....57
7.2 Conception du programme de sensibilisation....58
7.2.1 Groupes d'utilisateurs cibles....58
7.2.2 Messages ciblés....60
7.2.3 Contenu adapté de la sensibilisation....60
7.2.4 Moyens de communication adaptés....62
7.3 Diffusion du programme de sensibilisation....64
7.4 Evaluation du programme de sensibilisation....64
7.4.1 Besoin de sensibilisation....65
7.5 Maintenance sur le long terme....66

7.5.1 Fréquence du programme et des révisions 66
7.5.2 Contenu de la communication de sensibilisation 66
7.5.3 Nouveaux collaborateurs 66
7.6 Conclusion 67
8. Synthèse 68
Bibliographie 69
Annexe 1 : Canaux de communication proposés 73
Annexe 2 : Mail de réponse 78
Annexe 3 : Interviews des entreprises privées 79
Annexe 4 : Interviews à la Haute Ecole de Santé 85
Annexe 5 : Interviews à la Haute Ecole de Gestion 104
Annexe 6 : Plan – Phase 1 - Planification 116
Annexe 7 : Plan – Phase 2 – Conception 117
Annexe 8 : Plan – Phase 3 – Diffusion – Etape 1 118
Annexe 9 : Plan – Phase 3 – Diffusion – Etape 2 119
Annexe 10 : Plan – Phase 4 – Evaluation – Etape 1 120
Annexe 11 : Plan – Phase 4 – Evaluation – Etape 2 121
Annexe 12 : Plan – Phase 5 – Maintenance 122
Annexe 13 : Canaux de communication non adaptés 123
Annexe 14 : Affiches de sensibilisation 124

Liste des tableaux

Tableau 1 : Principes de sécurité fondamentaux de l'information....6
Tableau 2 : Vecteurs de risques engendrés par l'employé....12
Tableau 3 : Dimensions de la sensibilisation....18
Tableau 4 : Acteurs impliqués et leurs responsabilités....56
Tableau 5 : Groupes d'utilisateurs ciblés et les objectifs de sensibilisation....59
Tableau 6 : Messages à faire passer auprès des groupes cibles....60
Tableau 7 : Contenu de la sensibilisation adapté aux groupes cibles....61
Tableau 8 : Canaux de sensibilisation adaptés aux utilisateurs....63
Tableau 9 : Moyens d'évaluation de la campagne de sensibilisation....65

Liste des figures

Figure 1 : Sources d'incidents de sécurité en 2008....10
Figure 2 : Le top trois des menaces de sécurité en 2013....11
Figure 3 : Cycle d'apprentissage à la sécurité des informations....16
Figure 4 : Dimensions de la sensibilisation en quatre axes....17
Figure 5 : Manque de consciente suffisante de la part des employés....18
Figure 6 : La menace la plus importante en 2012....19
Figure 7 : Pourcentage de plan de sensibilisation dans les entreprises de 2006 à 2011....23
Figure 8 : Manque de professionnels qualifiés....24
Figure 9 : Evolution pour 2013 du budget pour la sensibilisation en entreprise....24
Figure 10 : Obstacle majeur en 2012....24
Figure 11 : La pyramide de la sensibilisation....25
Figure 12 : Processus de sensibilisation basée sur la norme ISO 27002:2005....29
Figure 13 : Cycle de vie d'un programme de sensibilisation selon Microsoft....30
Figure 14 : Cycle de vie d'un programme de sensibilisation, selon l'ENISA....31
Figure 15 : Cycle de vie d'un programme de sensibilisation....31
Figure 16 : Exemple d'affiches dans les lieux communs de l'entreprise....43

1. Introduction

L'idée de ce travail de Bachelor nous est venue dans le cadre de notre travail au sein du service informatique de la Haute Ecole de Santé de Genève. En effet, nous sommes souvent confrontés à des utilisateurs qui ne prêtent pas forcément attention à la sécurité de leur ordinateur ou de leurs documents.

Cette problématique, nous l'avons rencontrée durant nos études. En classe, les professeurs ont souvent mis le doigt dessus, en nous expliquant combien un système d'information est important au sein d'une entreprise, car il permet à celle-ci d'assurer ses activités stratégiques et opérationnelles.

Surtout qu'actuellement, toutes proportions gardées, avec les différents incidents de fuites d'informations dans les banques, les agences gouvernementales, et le récent incident[1] qui a eu lieu à la Haute Ecole de Gestion de Genève, les utilisateurs devraient y être sensibilisés.

1.1 Problématique

Alors pourquoi ne le sont-ils pas ? Est-ce que le service informatique donne des consignes pour sécuriser un ordinateur ? Est-ce que les ressources humaines expliquent comment sécuriser les informations ? Est-ce que tout simplement, ils ne font pas attention parce que les consignes sont trop contraignantes ? Ce sont des questions auxquelles nous souhaitons répondre en effectuant ce travail, tant par curiosité personnelle et mise en relation avec ce qui est étudié en cours, que dans le but de proposer une solution pour réduire l'écart de compréhension entre la direction, le service informatique et les utilisateurs du système d'information.

1.2 Méthodologie de travail

Pour mener à bien ce travail et répondre à notre problématique, il s'agit dans un premier temps de cerner le rôle et les enjeux de la sécurité du système d'information, afin de comprendre dans quel contexte la sensibilisation doit s'effectuer, et ainsi démontrer l'importance d'un système d'information pour une entreprise.

Ensuite, nous nous focaliserons notre travail sur le niveau humain de la sécurité. Nous définirons le facteur de risque humain, dans le but de déterminer ses spécificités, quel

[1] TONINATO, Aurélie. La Haute Ecole de gestion victime d'une grosse fraude : 270 élèves doivent repasser l'examen ! In : Tribune de Genève [en ligne]. Dernière modification le 21.02.2012. http://www.tdg.ch/geneve/actu-genevoise/haute-ecole-gestion-victime-grosse-fraude-270-eleves-doivent-repasser-lexamen/story/28574846

est son importance au sein d'une entreprise et comprendre pourquoi il existe des mesures humaines de sécurité.

Nous passerons ensuite à la sensibilisation, que nous analyserons et nous tenterons de comprendre pour quelles raisons il est important de sensibiliser les employés.

Puis, nous expliquerons quelles sont les méthodes recommandées par les organismes mondialement reconnus pour mener à bien une campagne de sensibilisation au sein d'une entreprise.

Enfin, nous sommes allés « sur le terrain » interviewer des collaborateurs dans différentes entreprises privées, ainsi que dans deux Hautes Ecoles Spécialisées pour recueillir leur point de vue et comprendre comment la sensibilisation est mise en place.

Pour finir, nous proposerons, avec les moyens préconisés par les organismes reconnus, une approche pour améliorer la sensibilisation au sein des deux Hautes Ecole Spécialisées de Genève.

Nous avons tenté dans la mesure du possible de rechercher des sources actualisées, dans un souci de réalisme et d'efficacité.

2. Rôle et enjeux du système d'information

2.1 L'information

Tout d'abord, il faut comprendre qu'une entreprise sans aucune forme d'information n'est pas une entreprise. En effet, s'est une composante intrinsèque à toute entité, c'est un flux de données vitales pour la bonne marche d'une entreprise. Nous pourrions comparer l'importance de l'information au système cardio-vasculaire d'un être vivant.

L'information[2] est au cœur de toutes activités stratégiques et opérationnelles, qui permet à une entreprise d'atteindre ses objectifs. Elle est non seulement générée à l'intérieur d'une entreprise, mais elle est aussi échangée avec l'extérieur de l'entité. Son rôle est d'aider, entre autre, à la réflexion, à la prise de décision, à la construction d'un savoir-faire, ou encore à l'exécution opérationnelle. Elle officie aussi comme mémoire des actions passées (Larbi, 2006). En d'autres termes, elle génère et fournit des éléments clés qui permettent l'activité et le développement d'une entreprise.

Par conséquent, pour que l'information puisse être utilisée à travers et à l'extérieur de l'entreprise et transmettre son savoir aux différents organes de l'entité, un système a été mis en place, c'est le système d'information.

2.2 Le système d'information

Un système d'information (SI) est un ensemble organisé de ressources humaines, organisationnelles, logiciels et matériels, permettant de gérer l'information qui est collectée, traitée, stockée, partagée, communiquée, sécurisée, archivée ou même détruite, nécessaire pour garantir les activités et l'atteinte des objectifs d'une entreprise. (Aïdonidis-Flückiger, 2013, p.9)

Si l'entreprise était un être vivant, nous pourrions comparer le fonctionnement et l'importance du SI au système nerveux. Il permet le traitement de l'information recueillie à tous les niveaux de l'entreprise et de prendre les décisions qui s'imposent grâce à elle.

Aujourd'hui, le SI est presque entièrement informatisé. Le système informatique est une composante cruciale du SI dans une entreprise. En effet, depuis plusieurs dizaines d'années, les utilisateurs du SI utilisent des ressources informatiques pour leur travail

[2] Bien que données et informations représentent des concepts différents, nous avons décidé de les grouper sous le terme général d'information.

quotidien. C'est devenu un outil majeur et usuel qui fait partie intégrante d'une entreprise.

Ce système informatique est composé d'un ensemble de moyens technologiques, comme la téléphonie, les réseaux, les logiciels, le matériel et les bases de données, permettant de gérer de manière électronique le SI d'une entité et de faciliter la transmission des informations à l'intérieur et à l'extérieur de celle-ci. (Aïdonidis-Flückiger, 2013, p.11)

2.2.1 Types de menaces

Mais comme pour tout système, un SI est vulnérable. C'est pourquoi, il est nécessaire de sécuriser au mieux celui-ci contre de potentielles menaces intentionnelles ou non.

Ces menaces sont de trois types distincts :

- les accidents ;
- les erreurs ;
- la malveillance.

Les accidents sont d'origine naturelle ou matérielle, comme une inondation ou un dysfonctionnement technique (Boulet, 2007). Ceux-ci détériorent ou provoquent généralement l'indisponibilité partielle ou totale du système.

Les erreurs, elles, sont d'origine humaine, comme les erreurs d'inattention, de négligence, ou encore d'incompétence (Boulet, 2007). Celles-ci n'engendrent pas forcément l'indisponibilité immédiate, mais peuvent compromettre une partie ou la totalité du système ou encore le rendre inaccessible durant un certain temps.

Le dernier type de menace est la malveillance. Elle aussi est d'origine humaine, mais celle-ci englobe les attaques logiciels, le vol d'information, ou encore le vandalisme sur le matériel de l'entreprise (Boulet, 2007). Ces attaques sont intentionnelles, et sont perpétrées dans le but de nuire à l'entité visée.

2.2.2 Conséquences

Ces différentes menaces peuvent engendrer des conséquences graves pour une entreprise. Si elles venaient à se concrétiser, elles porteraient atteinte :

- aux activités stratégiques et opérationnelles de l'entreprise ;
- à son savoir-faire ;
- à sa réputation et à son image, donc par extension à la confiance que lui portent ses partenaires commerciaux[3] (clients, sous-traitants ou fournisseurs).

De là, peuvent découler de lourdes pertes financières, des conséquences importantes sur le plan juridique ou encore mettre en danger les activités de l'entreprise, et donc par extension son existence (Boulet, 2007).

2.3 La sécurité du système d'information

> *« L'information constitue un bien important pour l'organisme; elle est à ce titre un élément important de l'activité de l'organisme et elle nécessite une protection adéquate. »* *(Norme ISO 27002 : 2005, p. viii)*

Comme nous l'avons expliqué au début de ce travail, une entreprise doit pouvoir assurer la valeur de ses informations, telles que ses informations commerciales, les bases de données de sa clientèle, de ses fournisseurs ou sous-traitants, ou encore ses secrets de fabrication. Elle doit aussi protéger son patrimoine ou encore son savoir-faire, afin de rester compétitive sur le marché économique et préserver sa réputation.

Pour pallier aux différents types de menaces établis auparavant, qui pèsent sur son système d'information, une entreprise doit mettre en place un ensemble de moyens techniques, organisationnels, juridiques et humains, pour protéger ses ressources et garantir ses activités. Ainsi, elle prévient les différents risques d'incidents au niveau physique, au niveau logiciel, niveau juridique, ainsi qu'au niveau humain (Calé, Touitou, 2007). Avec ces mesures, elle protège son SI et évite de lourdes pertes financières et d'importantes conséquences juridiques qui pourraient être néfastes à son activité.

En d'autres termes, l'objectif de la sécurité du système d'information (SSI) est d'éviter de mettre en péril la continuité des activités clés de l'entreprise.

2.3.1 Principes fondamentaux de la sécurité

L'entreprise doit assurer certains principes de sécurité fondamentaux pour les informations qu'elles gèrent quotidiennement, et ainsi certifier auprès de ses employés

[3] Par partenaires commerciaux nous désignons, tout au long de ce travail, les clients, les sous-traitants et les fournisseurs.

et partenaires commerciaux, de la véracité de celles-ci. Ces principes sont les suivants :

Tableau 1 : Principes de sécurité fondamentaux de l'information

Principes	**Explications**
Disponibilité	*« Qui permet de garantir l'accès à un service ou à des ressources. »*
Intégrité	*« Qui garantit que les données sont bien celles que l'on croit être, qu'elles n'ont pas été altérées [...]. »*
Confidentialité	*« Qui consiste à rendre l'information inintelligible à d'autres personnes que les seuls acteurs de la transaction. »*
Authentification	*« Qui consiste à assurer l'identité d'un utilisateur, c'est-à-dire à garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être. »*
Non-répudiation	*« Qui est la garantie qu'aucun des correspondants ne pourra nier la transaction. »*

(Pillou, Bay, 2005, p. 205-206)

2.3.2 Responsable de la sécurité du système d'information

> *« Le responsable de la sécurité du système d'information […] est l'auteur et le chef d'orchestre de la sécurité du système d'information de l'entreprise. » (Doucende, 2009)*[4]

L'entreprise nomme un responsable qui a la charge de protéger son SI. Pour cela, il doit mettre en place une politique de sécurité du système d'information qui tient compte de tous les processus métiers et leurs spécificités dans l'entreprise (Harle, Skrabacz, 2004). Le responsable s'assure que la politique est adaptée au SI de l'entreprise, qu'elle est appliquée par tous et garantit qu'elle reste efficace et pertinente pour les activités stratégiques et opérationnelles de l'entité. (Calé, Touitou, 2007)

En plus de rester à niveau du point de vue technologique, ainsi que d'avoir de bonnes connaissances des métiers de son entreprise, le responsable doit connaître la législation concernant le traitement des données informatiques et la protection de la personnalité de ses collaborateurs (CLUSIF, 2013). Ces connaissances doivent lui servir lors de la création de la politique de sécurité du système d'information de l'entreprise.

[4] DOUCENDE, Bruno. *Sécurité des Systèmes d'Information* [en ligne]. Livre Blanc. Marseille : Groupe 4, 4IM SAS, 2008. Page 29. http://www.globalsecuritymag.fr/IMG/pdf/Livre_Blanc_SSI_v1.pdf

2.3.3 Types de mesures de sécurité

« Le système d'information représente un patrimoine essentiel de l'entreprise, qu'il convient de protéger. » *(Pillou, Bay, 2005, p.205)*

Les mesures de sécurité dont nous avons parlé rapidement à la page précédente, sont mises en place dans le but de prévenir et d'empêcher du mieux possible, dans un premier temps, les menaces qui pèsent sur le SI d'une entreprise. Mais aussi dans un deuxième temps, sauvegarder et récupérer les données corrompues ou perdues selon l'incident et permettre la continuité de l'activité même en cas d'indisponibilité du système.

Ces mesures sont les suivantes :

- Les mesures techniques

  Ce sont des mesures tant au niveau matériel qu'au niveau logiciel qui sont intégrées au système informatique de l'entreprise pour protéger le SI. Elles permettent de filtrer les différentes menaces logicielles, d'éviter des vols d'information, ou d'empêcher une intrusion. Ces mesures se traduisent par la mise en place entre autres d'antivirus, de pare-feu, de détection d'intrusion, de cryptage, ou encore de clé d'accès électronique. (Calé, Touitou, 2007)

- Les mesures organisationnelles

  Ce sont des mesures de management. Elles expliquent comment établir une culture de la SSI au sein de l'entreprise, comment gérer la sécurité, comment réagir en cas d'incident ou encore comment récupérer les informations, afin d'assurer la continuité des activités stratégiques et opérationnelles de l'entreprise. Ces mesures se traduisent par une politique de sécurité du système d'information, une gestion des risques, ou encore la classification du degré de confidentialité. (Calé, Touitou, 2007)

- Les mesures juridiques

  Ce sont des mesures légales applicables à la sécurité du SI. Ces dernières sont mises en place afin d'éviter que sur le plan juridique l'entreprise soit tenue responsable en cas d'incident. L'entreprise doit établir une politique de gestion juridique du risque informatique. Celle-ci doit se baser sur une charte d'utilisation des outils informatiques définissant les droits et les obligations de chaque utilisateur, la désignation d'un responsable chargé de la SSI, la souscription de contrats d'assurance adaptés et une évaluation régulière des risques et des mesures de sécurité appropriées. (Calé, Touitou, 2007)

- Les mesures humaines

  Ce sont des mesures qui visent à informer, former et sensibiliser les employés de l'entreprise, tant de manière préventive que de manière rétroactive. Elles permettent aux utilisateurs du SI et par extension du système informatique, de prendre conscience des différents types de risques qu'ils font encourir au SI de leur entreprise par un mauvais usage de la technologie (Calé, Touitou, 2007). Ces mesures doivent en principe être transmises lors de l'engagement de l'employé, ainsi que lors de programmes de sensibilisation à la SSI de l'entreprise dédiés aux collaborateurs. (Norme ISO 27002:2005)[5]

C'est par ce type de programme qu'une entreprise peut réduire le facteur de risque humain qui pèse sur son SI. Comme l'explique un professionnel dans le domaine de la sécurité des systèmes d'information :

> *« Sensibiliser tout simplement les collaborateurs aux cybers menaces pouvant les impacter […] et aux moyens de se défendre contre ces dernières aura également un impact fort sur la sécurité de l'entreprise. Certaines menaces parmi les plus virulentes [..] seront mieux repoussées par des employés sensibilisés. » (Gratiolet, 2013)[6]*

La suite de ce travail est dédiée à la définition du facteur de risque humain et aux mesures de sécurité au niveau humain que nous pouvons mettre en place pour aider à réduire ce risque.

[5] Voir le chapitre Méthodologie, concernant la norme 27002:2005 p.25

[6] GRATIOLET, François. Sensibilisation à la cyber-sécurité : se prémunir des vulnérabilités d'origine humaine. In : Le Cercle – Les Echos [en ligne]. 2013. http://lecercle.lesechos.fr/entrepreneur/tendances-innovation/221177184/sensibilisation-a-cyber-securite-premunir-vulnerabilites

3. Le facteur risque humain

Mais avant d'en venir aux solutions pour rendre un employé acteur de la sécurité au sein de son entreprise, intéressons-nous au pourquoi. Pourquoi l'employé est-il un facteur de risque au sein d'une entreprise ? Qu'est-ce qu'un employé peut bien faire pour rendre vulnérable le SI d'une entreprise et attenté à la sécurité de l'information ? Ce sont des questions auxquelles nous allons tenter de répondre dans ce chapitre.

3.1 Définition

Tout d'abord, que signifie un facteur de risque humain : *« […] source de risque [...] dont le déclenchement est dû à l'action de l'homme. » (Wikipédia, 2013)*

Ce facteur de risque peut être soit involontaire de la part d'un être humain, comme une erreur due au stress, à la fatigue ou encore dû à l'intervention d'un tiers. Soit volontaire, c'est-à-dire que l'acte est fait de manière consciente ou délibérée. (Wikipédia 2013)

Nous pouvons donc déterminer, selon ces deux définitions, que le facteur de risque au niveau humain, veut dire de manière simple : *« une source de risque potentielle déclenchée par l'action de l'homme de manière volontaire ou involontaire. »*

Pour terminer, ce facteur de risque a deux origines :

- **Endogène :** c'est-à-dire qu'il est généré par l'organisation elle-même ou à l'intérieur du périmètre qu'elle contrôle ; (Wikipédia, 2013)
- **Exogène :** c'est à qu'il est généré à l'extérieur du périmètre de contrôle de l'entreprise. (Wikipédia, 2013)

Nous expliciterons par des exemples ces origines au dernier point de ce chapitre.

3.2 L'importance de ce risque

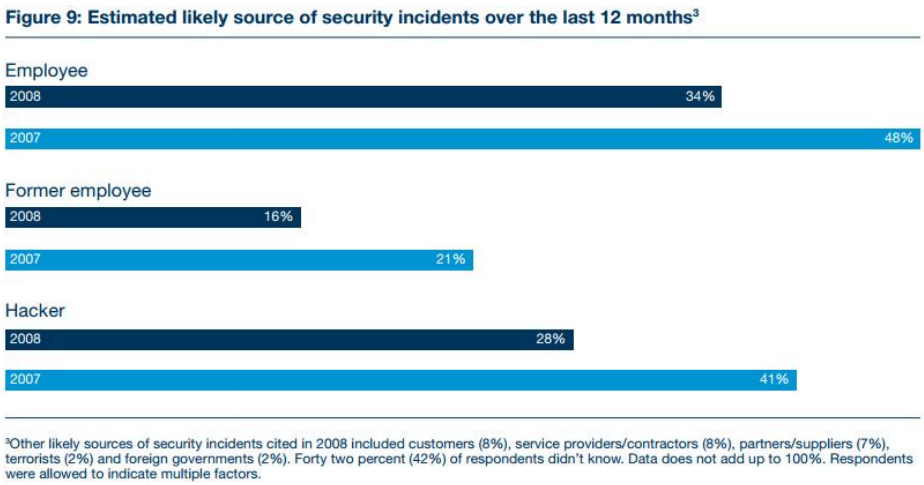
En 2012, le directeur technique de Check Point Software Technologies[7], établit que le facteur humain est l'une des trois sources principales de vulnérabilités dans une entreprise. Le directeur explique qu'un employé peut commettre des erreurs ou faire preuve de négligence, ou encore délibérément organiser une fuite d'informations.

Ce qui reprend les notions que nous venons d'établir, c'est-à-dire qu'un employé est un facteur de risque qui par ses actes involontaires ou volontaires peut rendre vulnérable la sécurité des informations d'une entreprise. D'ailleurs, le CLUSIR explique dans l'une de ces présentations : *« Le maillon faible de la sécurité informatique est souvent le facteur humain »*[8]. Et nous met en garde :

> *« La principale menace contrairement à ce que l'on pourrait penser, ne vient pas de l'extérieur mais il s'agit bien du facteur humain c'est-à-dire de l'utilisateur [à l'intérieur de l'entreprise]. »* *(CLUSIR, 2005, p.4)*

Avec ces explications d'experts en sécurité, nous pouvons donc estimer qu'une entreprise ne pense pas toujours qu'à l'intérieur même de ses murs, il peut y avoir un risque intentionnel ou non, de la part d'un collaborateur qui provoquerait des conséquences dramatiques pour son activité. En effet, en 2008, selon le sondage publié par PricewaterhouseCoopers, 50% des incidents de sécurité provenaient des collaborateurs ou ex-collaborateurs.

Figure 1 : Sources d'incidents de sécurité en 2008



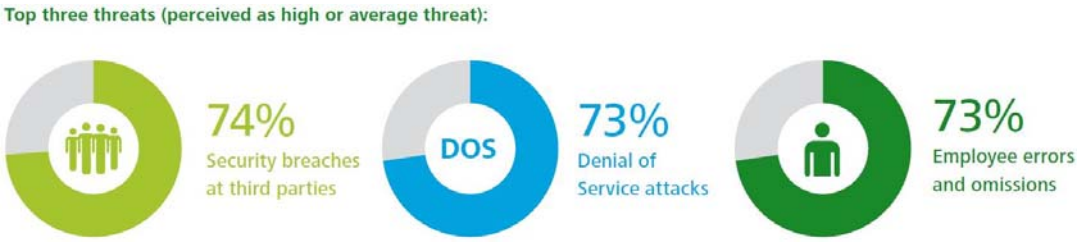
(PricewaterhouseCoopers, 2008, p.27)

[7] L'entreprise Check Point Software Technologies est leader mondial de la sécurité informatique. Sécurité informatique – Prévention des menaces en entreprise. Info Expoprotection. 2012.

[8] GOMAS, Olivier, RAISIN, Yves, ROZIER, Richard. Le facteur humain. In : *CLUSIR Rhône-Alpes* [en ligne]. Page 3. http://www.clusir-rha.fr/sites/default/files/upload/Lyon/SSI/CLUSIR_FACTEUR%20HUMAIN_161903.pdf

En 2013, l'employé est toujours une des principales sources d'incidents pour l'entreprise, selon une étude effectuée par Deloitte. Ce sont les erreurs et les omissions des employés qui à hauteur de 73%, représentent une des trois principales menaces pour l'entité.

Figure 2 : Le top trois des menaces de sécurité en 2013



(Deloitte, 2013, p.8)

Dans son rapport de 2012, la centrale fédérale d'enregistrement et d'analyse pour la sûreté de l'information indique que : « *les mécanismes techniques de sécurité, bien qu'indispensables, n'offrent pas une protection à 100 %.* » en parlant du nouvel usage fait par les employés des technologies professionnelles de l'information, à titre personnel. Nous pouvons donc déduire que même si une entreprise protège son SI par des mesures techniques, celles-ci ne permettent pas apparemment de contrer les actions de l'être humain sur son système d'information. (MELANI, 2012, p.26)

Par exemple, un employé peut faire des erreurs d'inattention en discutant avec une personne extérieure ou en envoyant des informations sensibles par erreur à un client ou un fournisseur, surtout si celui-ci est soumis à un stress quelconque à un moment donné. Il peut faire des erreurs dans la manipulation d'un logiciel, ou d'un équipement, parce qu'il n'a pas les connaissances ou la formation nécessaires pour les utiliser. Ou encore faire preuve de négligence en laissant trainer des informations sensibles sur un copieur, ou en divulguant des informations confidentielles autour de lui sans penser aux conséquences que cela peut avoir. Enfin, un employé qui a un quelconque grief contre son employeur ou un collègue peut commettre un vol, ou vandaliser des équipements stratégiques dans le but de nuire à l'un des deux. Ces exemples repris par beaucoup de professionnels dans le domaine de la SSI, dont le directeur technique Europe de Check Point Software Technologies, démontrent bien que l'humain est complexe et des mesures de sécurité ne peuvent être restreintes à des mesures techniques.

3.3 Les vecteurs de menaces

Tentons donc de comprendre pourquoi un employé fait toujours partie en 2013 d'une des trois plus importantes menaces pour le SI d'une entreprise.

Deloitte, dans son étude, avance une réponse. L'entreprise explique que les utilisateurs sont les premiers à manipuler quotidiennement les informations de l'entreprise. De plus, avec l'évolution de la technologie, et l'utilisation qui en est faite par les employés, cela ne fait qu'augmenter les chances d'introduction de nouveaux risques pour la sécurité de l'information. (Deloitte, 2013, p.10)

Alors pour préciser ce que Deloitte entend par là, nous allons passer en revue les différents vecteurs par lequel un employé peut provoquer un incident durant son travail, sans s'en rendre compte.

Monsieur Henrique Marques, avait déjà établi en 2006 pour son travail de Bachelor, un premier tableau qui liste et explique les principaux outils qu'utilise un employé dans son environnement professionnel et qui peuvent être vecteurs de risques pour une entreprise. Néanmoins, nous nous sommes permis de compléter le tableau par des outils ou des conséquences qui se sont ajoutés au gré de l'évolution technologique et sociale, à la liste des outils professionnels utilisés au sein d'une entreprise, comme évoqués par les responsables de la sécurité.

Tableau 2 : Vecteurs de risques engendrés par l'employé

Vecteurs	**Conséquences**
Messagerie	Recevoir un courrier électronique d'un expéditeur inconnu et en ouvrir les pièces jointes ou cliquer sur des liens se trouvant dans le message, peut générer des risques d'attaque. S'abonner à diverses newsletters avec son adresse électronique professionnelle peut également générer des spams ou provoquer une faille dans la protection du système.
Internet	Naviguer sur des sites non professionnels, tel que des pages douteuses, peut générer des virus ou des logiciels espions.
Réseaux sociaux	Partager sa vision personnelle de son entreprise sur les réseaux sociaux, peut nuire à l'image ou à la réputation d'une entreprise. De plus, selon la nature des messages, cela peut engendrer de graves conséquences stratégiques et sécuritaires pour une entité et ses employés. Naviguer sur les réseaux sociaux et cliquer sur des liens douteux, peut aussi provoquer l'infection d'un ordinateur.
Applications personnelles	Télécharger des applications sur internet ou via un autre support personnel, peut introduire au sein de l'entreprise des virus ou des logiciels espions entre autres.

Ordinateur personnel	Connecter un ordinateur personnel sur le réseau informatique de l'entreprise, peut aussi introduire ce genre de menaces. Soit si l'ordinateur lui-même est infecté par un type de virus, soit si celui-ci est sous contrôle d'un individu malveillant qui peut générer une attaque de l'extérieur[9].
Supports personnels	Brancher un média tel que Smartphone, tablette, lecteur de musique, clé USB, disque externe, peut aussi transmettre des infections au SI de l'entreprise, car il se peut qu'un de ces outils ait été infecté auparavant.
Ingénierie sociale	Donner des informations concernant l'entreprise à une personne extérieure à celle-ci, peut compromettre la SSI et permettre une attaque contre l'entité.
Copieur	Envoyer à l'impression un document et ne pas rester à côté de celui-ci jusqu'à récupérer le document en main propre, peut porter atteinte à la confidentialité des informations et engendrer d'importante conséquences.
Poubelle	Ne pas détruire de documents confidentiels avant de les jeter à la poubelle, peut nuire à l'entreprise, et engendrer comme ci-dessus d'importantes conséquences.
Casier ouvert pour la correspondance	Mettre des documents importants, ou confidentiels dans un casier ouvert, peut nuire à la confidentialité des informations, ainsi qu'au SSI.
Hors du lieu de travail	Travailler à l'extérieur de l'entreprise peut poser des problèmes de confidentialité ou de disponibilité des informations. Des documents peuvent traîner, un individu peut regarder par-dessus l'épaule de l'employé ou celui-ci peut oublier des documents importants sur place.
Employé	Faire une erreur, avoir un mot de passe peu complexe, perdre ou oublier une carte/clé d'accès ou un support de stockage contenant des informations sensibles, peut provoquer de graves conséquences. De plus, un employé contrarié envers son entourage professionnel, peut attaquer, voler, partager, détruire ou altérer des informations ou du matériel appartenant à son employeur dans le but de se venger ou satisfaire son besoin de reconnaissance.

(Marques, 2006, p.9)

Après avoir listé les différentes voies par lesquelles un employé peut provoquer un incident, ainsi que les conséquences que cela peut engendrer sur le SI de l'entreprise, nous pouvons donc en conclure qu'un employé est effectivement une menace élevée pour l'entreprise. D'autant plus qu'une mauvaise manipulation est imprévisible pour une entreprise, surtout si un employé n'est pas informé de l'impact de ses

[9] Pour illustrer, voici un exemple d'intrusion via un ordinateur portable personnel :

Deloitte. *Situation de cyber attaque susceptible de menacer votre entreprise* [en ligne]. http://www.deloitte-france.fr/video/CPL/video.htm, durée : 4 min

manipulations sur le SI. Du reste, Deloitte explique dans son étude, que l'élément humain est l'une des plus grandes sources de risque, aussi bien que la plus difficile à contrôler. (Deloitte, 2013, p.10)

Bien évidemment, cela ne veut pas dire qu'à chaque fois qu'un collaborateur fera preuve d'inattention dans l'utilisation de ces outils, cela engendra un incident. Mais le risque existe par ces vecteurs et se répercute sur la confidentialité, la disponibilité, l'intégrité de l'information, la réputation de l'entreprise, la sécurité du personnel, ainsi que sur l'ensemble du SI, qui se voient compromis avec ce genre d'utilisation. C'est pourquoi des mesures de sécurité au niveau des ressources humaines existent pour sécuriser le SI de l'entreprise.

4. La sensibilisation

Dans ce chapitre nous allons expliquer en détail ce que signifient ces mesures de sécurité humaines évoquées précédemment, ainsi que les avantages amenés par la sensibilisation aux employés.

4.1 Définition

Si nous prenons le Wikitionnaire, celui-ci a plusieurs définitions à proposer pour définir la sensibilisation, mais deux d'entre elles ont retenu notre attention.

La première est la suivante : « *C'est l'action de rendre attentif à quelque chose pour lequel on ne manifestait pas d'intérêt auparavant.* » (Wikitionnaire, 2013)

La seconde définit la sensibilisation du point de vue biologique, ce qui nous donne un complément à notre première définition et nous rapproche de la réaction de l'être humain.

> *« Processus par lequel un stimulus qui, au préalable, ne déclenche aucune réponse particulière, acquiert un pouvoir de déclenchement d'une réponse, soit par simple répétition, soit par présentation d'un autre stimulus. »*

(Wikitionnaire, 2013)

Avec ces deux différentes définitions, nous pensons pouvoir donner une définition générale et complète de ce qu'est la sensibilisation.

> *« C'est un processus par lequel un stimulus, qui auparavant ne déclenchait aucune réaction ou intérêt, permet de rendre réceptif à un événement précis, à force de répétition. »*

Maintenant, plaçons cette définition dans le contexte professionnel, pour comprendre ce que signifie sensibiliser un employé à la sécurité des informations de son entreprise. Pour cela, nous avons recherché une explication auprès d'une entité reconnue, l'European Network and Information Security Agency[10] (ENISA).

Selon elle, la sensibilisation tente de modifier le comportement et les pratiques des collaborateurs face à la sécurité de l'information, dans le but d'en faire un atout pour l'entreprise. L'ENISA précise que la sensibilisation doit s'effectuer de manière continue, en utilisant un large panel de méthodes de communication, et constitue une partie de la stratégie de sécurité dans une entreprise.

[10] L'ENISA est l'Agence Européenne chargée de la sécurité des réseaux et de l'information.

4.2 Dimensions

Pour mener à bien ce processus qu'est la sensibilisation, l'ENISA distingue deux aspects :

- la sensibilisation ;
- la formation.

C'est-à-dire qu'elle propose une stratégie sur deux dimensions pour rendre attentif les utilisateurs à la sécurité des informations, pour que la sensibilisation porte ses fruits dans la stratégie de la SSI de l'entreprise. Elle l'explique d'ailleurs en ces termes :

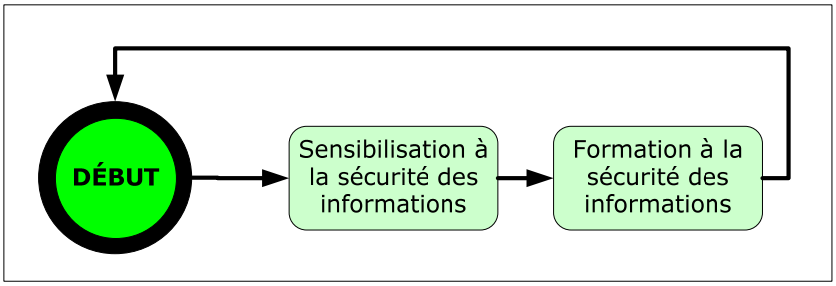
> *« La formation vise donc à enseigner à une personne des aptitudes lui permettant de remplir une fonction spécifique, tandis que la sensibilisation cherche à fixer l'attention d'une personne sur un point précis ou un ensemble de points. Les aptitudes acquises durant la formation reposent sur la sensibilisation, notamment sur les notions élémentaires de sécurité et le matériel de base. »*
>
> (ENISA, 2008, p.13)

Nous avons constaté qu'elle n'est pas la seule à proposer ces deux aspects pour mener à bien un programme de sensibilisation. Effectivement, Microsoft fait aussi cette distinction. Il explique la différence entre sensibiliser et former comme cela :

> *« Le principal objectif du développement de la sensibilisation à la sécurité des informations consiste à modifier le comportement du personnel en renforçant des pratiques professionnelles acceptables vis-à-vis de la sécurité. Pour parvenir à cet objectif, il est indispensable de faire comprendre les aspects de la sécurité des informations et de permettre aux individus de les appliquer. »*
>
> (Microsoft, 2006)

Et l'illustre comme cela :

Figure 3 : Cycle d'apprentissage à la sécurité des informations



(Microsoft, 2006, p.5)

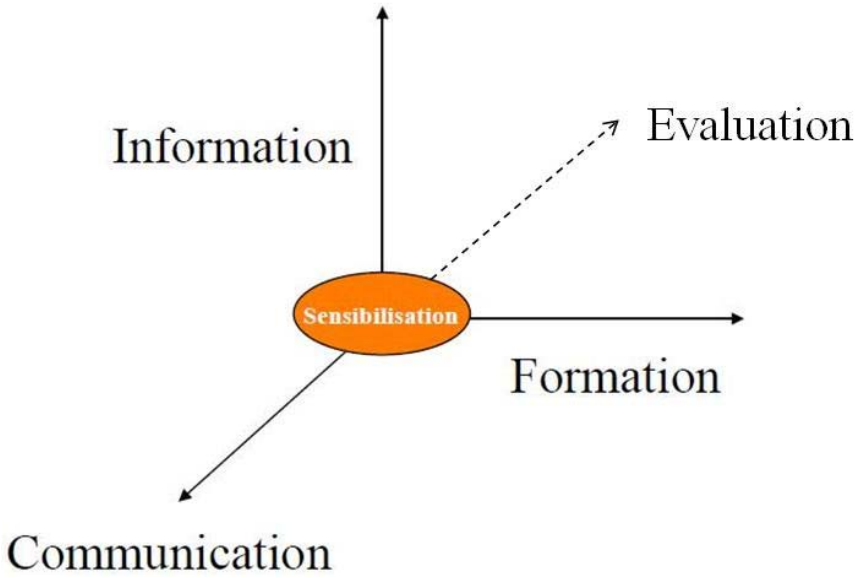
Nous constatons, en outre, que l'ENISA[11] et Microsoft[12] proposent de mettre en place un moyen d'évaluer ce processus de sensibilisation. Le but est d'apprécier l'impact que cette campagne de sensibilisation a sur les employés de l'entreprise, ainsi que de déterminer le processus de continuité et de mises à jour nécessaires pour le bon déroulement du programme.

D'ailleurs, Monsieur Hauri, professeur à la Haute Ecole de Gestion de Genève, en Gouvernance de la sécurité du système d'information, intègre aussi l'évaluation dans le processus de sensibilisation.

Cependant, le professeur Hauri, décompose la dimension de « sensibilisation », proposée par les deux organismes, en deux axes distincts. En effet, il propose les quatre axes suivants :

- l'information ;
- la communication ;
- la formation ;
- l'évaluation.

Figure 4 : Dimensions de la sensibilisation en quatre axes



(R. Hauri, 2011, p.10)

[11] ENISA. Le nouveau guide utilisateur : comment améliorer la sensibilisation à la sécurité de l'information. 2008, 110p. http://www.enisa.europa.eu/publications/archive/new-users-guide-fr

[12] Microsoft. Facteurs clés pour le développement de programmes efficaces de sensibilisation et de formation à la sécurité des informations. In : Sensibilisation à la sécurité [en ligne]. 2006. http://technet.microsoft.com/fr-fr/security/cc165442.aspx

Selon eux, les résultats générés par l'évaluation donneront les clés pour améliorer ou redéfinir la politique de sensibilisation, d'après les nouvelles menaces apparaissant avec l'évolution de la technologie et de l'entreprise.

Expliquons ce que signifient ces différents axes stratégiques dans un processus de sensibilisation, afin de mieux comprendre leur rôle sur les utilisateurs.

Tableau 3 : Dimensions de la sensibilisation

Dimensions	Explications
Information	Tout d'abord, il s'agit d'informer l'utilisateur des dangers existants dans le cadre de son travail.
Communication	Ensuite, il s'agit de le sensibiliser face aux risques que ces menaces peuvent engendrer pour l'entreprise ou sur son travail et de lui expliquer ce qu'il doit faire pour les éviter.
Formation	Enfin, il s'agit de lui enseigner par des moyens qui l'impliquent consciemment dans le processus de sensibilisation global.
Evaluation	Finalement, il s'agit de mettre en place un système d'évaluation continu qui permet de mesurer l'impact que cette campagne a eu sur les employés et la sécurité du système d'information, pour ultérieurement l'améliorer.

(R. Hauri, 2011, p.10)

4.3 Pour quelles raisons sensibiliser

Ici, nous allons démontrer pourquoi il est nécessaire de sensibiliser les employés.

4.3.1 Peu conscients de l'importance de la sécurité

Comme nous l'avons vu au chapitre précédent, les employés ne sont pas forcément conscients que leurs actes peuvent mettre en péril le SI et par extension l'entreprise. D'ailleurs, pour appuyer ce fait, l'étude menée par Deloitte pour 2013, à montrer que dans 70 % des entreprises, il y a un manque certain de conscience de la part des employés quant à la sécurité des informations qu'ils manipulent. Du reste, Deloitte explique ensuite que les employés sans une connaissance suffisante de la sécurité des informations, peuvent mettre une entreprise en péril.

Figure 5 : Manque de consciente suffisante de la part des employés

(Deloitte, 2013, p.10)

Pour appuyer ce fait, Ernst and Young explique que dans 37% des entreprises sondées, les responsables de la sécurité estiment que la menace qui a le plus augmenté pour l'entreprise, est l'inconscience et la négligence des employés. La perte d'informations confidentielles causée par l'inconscience de certains employés a augmenté de 25% en 2012, selon le rapport publié par la banque.

Figure 6 : La menace la plus importante en 2012

(Ernst and Young, 2012, p.20)

Rappelons qu'au chapitre précédent[13], selon Deloitte, la manière dont les employés utilisent les nouvelles technologies, introduit de nouveaux risques au sein de l'entreprise.

Pour appuyer ce faite les responsables en charge de la sécurité interrogés par Ernst and Youg, explique que selon eux c'est dû à la prolifération des appareils mobiles personnels et des réseaux sociaux, utilisés tant comme outils professionnels que comme moyen de récréation.

Pour eux, la frontière entre la vie professionnelle et la vie personnelle s'est floutée avec l'évolution des technologies de l'information. Par conséquent, nous pourrions en déduire alors, qu'il y aurait donc une nouvelle menace en plus de l'inconscience des collaborateurs, depuis quelques temps.

4.3.2 Nouvelle génération, nouveaux risques

Nous pourrions faire un parallèle entre ce que les responsables chargé de la sécurité des systèmes d'information estiment et la vision qu'expose ce livre blanc *« Sensibilisation à la sécurité de l'information 2.0 »*[14] concernant l'émergence en entreprise d'une nouvelle génération d'employés connectés aux nouvelles technologies de l'information.

Selon les auteurs de ce document, cette génération comprend les employés nés durant ces trente dernières années, donc avec les nouvelles technologies de l'information telles que nous les connaissons. Ceux-ci sont informés sur les

[13] Voir page 11.

[14] BENNASAR, Matthieu, BRIGAUD, Julien, COMBES, Létitia. *Sensibilisation à la sécurité de l'information 2.0* [en ligne]. Livre Blanc. PARIS : LEXSI – INNOVATIVE SECURTIY, 2013. Page 6 https://www.lexsi.fr/sites/default/files/publications/lb_sensibilisation_a_la_securite_de_linformation_2.0.pdf

Toutes les citations de ce point proviennent de la page 6 de ce livre blanc.

technologies, et sont de plus en plus nombreux dans les entreprises. D'après les auteurs, ils révolutionnent la manière de travailler avec le système d'information.

En effet, ceux-ci amènent donc un élément pour étayer la vision des responsables chargé de la sécurité, en expliquant que cette génération raisonne différemment des générations précédentes parce qu'elle a évolué avec les nouvelles technologies de l'information. D'après les auteurs, ils surestiment leurs connaissances en matière de sécurité des systèmes d'information, car ces utilisateurs pensent mieux maitriser les outils technologiques que leurs collègues de l'ancienne génération. *« [Ils ont] l'impression de maitriser les SI et ne se donnent pas la peine de lire les recommandations de sécurité. »* Ils n'estiment, donc, pas avoir besoin de respecter la politique de sécurité mise en place par l'entreprise, bien qu'ils en soient informés surtout s'ils ne la comprennent pas. Les auteurs expliquent que ces utilisateurs souhaitent comprendre pourquoi ils doivent appliquer ces règles, sinon ils sont les premiers à la contourner. *« [Ils] sont bien connus pour s'interroger sans cesse sur la raison d'être des choses »*. Enfin, ces utilisateurs ont toute une panoplie de médias connectés qu'ils utilisent dans leur vie professionnelle et personnelle, ce qui peut nous laisser penser qu'ils ont une autre approche des technologies que leurs collègues et traitent donc l'information autrement, cela crée donc une nouvelle faille dans le système de sécurité de l'entreprise.

En conséquence, comme les auteurs de ce document le soulignent judicieusement et ainsi rejoignent ce que pensent les responsables chargé de la sécurité des systèmes d'information en entreprise interrogés par Deloitte, cela entraine de nouveaux risques pour les entreprises. Ces explications font échos à ce que nous avons constaté dans les pages précédentes. Pour finir, ces mêmes auteurs estiment que les entreprises doivent s'adapter et tenir compte de ces différences générationnelles et de l'évolution des technologies pour ajuster leur sécurité. Par conséquent, toujours selon eux, cela implique donc de proposer une sensibilisation à la sécurité des systèmes d'information qui tient compte de ces explications.

4.4 Intégrer la sensibilisation dans le processus de sécurité

Il apparait donc, après ces observations, indispensable d'intégrer la sensibilisation dans la sécurité des systèmes d'information. Nous avons donc effectué quelques recherches afin d'apprécier ce qu'en disent les professionnels dans ce domaine. Nous avons constaté, effectivement, qu'un grand nombre d'organismes expliquent qu'il ne faut pas oublier la sensibilisation et la formation des utilisateurs dans le processus de sécurité des systèmes d'information.

Trois organismes français, parmi d'autres, prennent en compte ce point dans les documents qu'ils ont établit, dans le but qu'ils servent de guide pour les entreprises.

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) propose un « *Guide d'hygiène informatique* » à l'attention des responsables informatiques pour les aider à assurer la sécurité de leurs systèmes d'information.

> *« Règle 39 - Sensibiliser les utilisateurs aux règles d'hygiène informatique élémentaires. »*[15]

Elle énumère 40 règles, dont parmi elles, une règle qui vise la sensibilisation des utilisateurs du système à l'aide d'une charte informatique à faire signer. De plus, sur son site internet, nous pouvons trouver de nombreux conseils concernant les points à sécuriser et les messages à faire passer auprès des utilisateurs.

La Commission nationale de l'informatique et des libertés (CNIL) propose elle aussi un « *Guide La sécurité des données personnelles* » qui tout comme celui de l'ANSSI permet d'aider les responsables à vérifier et assurer les bases de la sécurisation dans leur entreprise. Ce guide énumère 17 points à prendre en compte, dont le troisième propose des précautions élémentaires en matière de sensibilisation, une structure pour une charte informatique, averti sur ce qu'il ne doit pas être fait et ce qui pourrait être mis en place en plus des propositions précédentes.

> *« Il convient de veiller également à ce que les utilisateurs soient conscients des menaces en termes de sécurité, ainsi que des enjeux concernant la protection des données personnelles. »*[16]

---

15 DUVAUCHELLE, Antoine pour l'Agence nationale de la sécurité des systèmes d'information. Guide d'hygiène informatique [en ligne]. 1ère éd. Paris : ANSSI, 2013. Page 43. http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf

16 COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES. Guide – La sécurité des données personnelles [en ligne]. Edition 2010. Inconnu : CNIL, 2010. Page 11. http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Guide_securite-VD.pdf

Le Centre national de la recherche scientifique (CNRS) a établit un document *« Politique de Sécurité des Systèmes d'Information (PSSI) »* où il explique au chapitre *« Principes de mise en œuvre de la PSSI »*, *« La formation, la sensibilisation et l'information des différents acteurs […] de l'entité sont cruciales pour la sécurité. ».*[17]

De plus, sur internet un grand nombre d'entreprises expliquent aussi qu'il est important de sensibiliser ces employés afin d'éviter un incident. Parmi celles-ci nous citerons Cyberworld Awarness & Security Enhancement Services (Cases), une entreprise luxembourgeoise, explique à l'attention des petites et moyennes entreprises sur son site internet qu'il est important de prendre des mesures de sensibilisation et appuie sur le fait que les mesures techniques ne sont pas les seules en matière de sécurité. En outre, elle explique de manière plus exhaustive ce qu'est la sensibilisation et proposent des exemples d'affiches pour informés ses employés.

> *« Penser à sensibiliser et former la totalité de vos employés. L'adoption des bonnes mesures comportementales par l'ensemble du personnel est une mesure extrêmement importante. En effet, il s'agit souvent de déployer davantage d'efforts au niveau organisationnel et comportemental qu'au niveau technique pour augmenter la sécurité de vos informations de manière efficace. »*[18]

[17] ILLAND, Joseph pour le Centre national de la recherche scientifique. Politique de Sécurité des Systèmes d'Information [en ligne]. 1ère éd. Inconnu : CNRS, 2006. Page 18. http://www.dgdr.cnrs.fr/fsd/securite-systemes/documentations_pdf/securite_systemes/pssi-v1.pdf

[18] CYBERWORLD AWARENESS & SECURITY SURVEY ENHANCEMENT SERVICES. Se protéger [en ligne]. https://www.cases.lu/fr/la-sensibilisation-et-la-formation.html

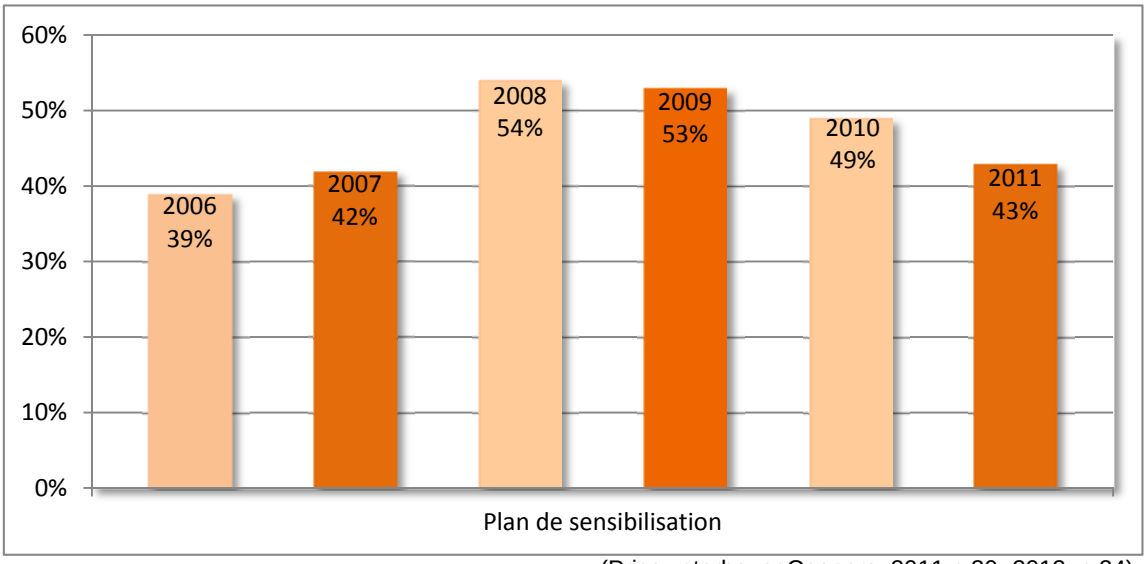
4.5 Statistiques actuelles en entreprise

Faisons maintenant un tour d'horizon concernant l'état de la sensibilisation dans les entreprises au niveau mondial, selon différents rapports de statistiques établis entre 2011 et 2013.

4.5.1 Baisse des programmes de sensibilisation

Selon les rapports de PricewaterhouseCoopers 2011 et 2012, nous pouvons constater qu'il y a une nette réduction du taux de mise en place d'un plan de sensibilisation, ces trois dernières années. Le rapport de 2011 évoque de multiples facteurs. Nous pourrions alors penser cette baisse est en partie due à la crise financière qui a commencé en 2008.

Figure 7 : Pourcentage de plan de sensibilisation dans les entreprises de 2006 à 2011



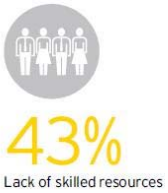
(PricewaterhouseCoopers, 2011 p.30 -2012, p.24)

Ernst and Young, apporte une autre proposition concernant cette baisse de budget. Selon son rapport, les entreprises ne jugent plus que ce soit l'une de leurs priorités absolues. En fait, elles estiment faire ce qu'il faut dans ce domaine, et c'est pour cela qu'elles se concentrent sur d'autres priorités en termes de mesures de sécurité.* Dans son rapport, la mesure de sensibilisation des employés est placée au dix-septième rang des priorités en termes de sécurité pour les entreprises en 2012, avec seulement 9% d'entre elles qui en font une de leur priorité (Ernst and Young, 2012, p.9). Alors que nous avons constaté auparavant que tous les chiffres démontrent qu'il serait judicieux d'augmenter les programmes de sensibilisation dans les entreprises.

4.5.2 Personnel dédié

Un programme de sensibilisation ne peut être efficace, qu'avec une formation adéquate des collaborateurs à la SSI. Dans le rapport d'Ernst and Young, 43% des entreprises expliquent que l'obstacle le plus important pour former les utilisateurs, en 2012, est le manque de professionnels qualifiés dans le domaine de la SSI.

Figure 8 : Manque de professionnels qualifiés



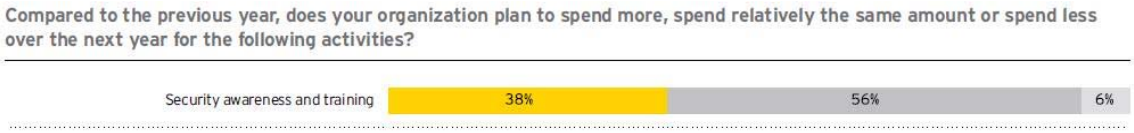
(Ernst and Young, 2012, p.20)

En effet, ceux-ci sont coûteux et cela a conduit, selon PricewaterhouseCoopers, à une diminution des équipes dédiées aux programmes de sensibilisation, de 51% en 2011 à 47% en 2012. (PricewaterhouseCoopers, 2013, p.20)

4.5.3 Budget

Une meilleure nouvelle pour 2013, 56% des entreprises maintiendront leur budget de l'année précédente concernant les mesures de sensibilisation, 38% augmenteront leur budget et seulement 6% reverront leur budget à la baisse. Ces chiffres nous laisser penser à une reprise économique pour une partie d'entre elles et donc à une plus grande capacité budgétaire pour augmenter les mesures de sensibilisation.

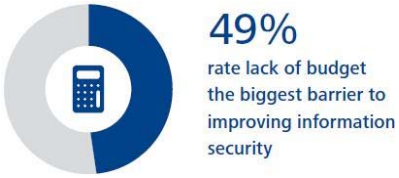
Figure 9 : Evolution pour 2013 du budget pour la sensibilisation en entreprise



(Ernst and Young, 2012, p.19)

Néanmoins, l'obstacle majeur à l'amélioration de la sécurité de l'information continue, en 2012, reste le manque de budget. Cela a été cité par 49% des entreprises interrogées par Deloitte.

Figure 10 : Obstacle majeur en 2012



(Deloitte, 2013, p.7)

4.6 Conclusion

En conclusion, comme nous l'avons vu, les utilisateurs eux-mêmes représentent une grande partie du problème, mais aussi de la solution lorsqu'il s'agit de sécuriser l'information utilisée au sein d'une entreprise. Ainsi, l'approche que nous avons décrite, permet d'informer l'utilisateur, de lui permettre d'appréhender les risques, et finalement d'en faire un utilisateur avertis.

Figure 11 : La pyramide de la sensibilisation

(R. Hauri, 2011, p.10)

D'ailleurs, Hapsis le confirme et nous permet de clore ce chapitre, en nous expliquant que l'employé est un des maillons crucial de la chaîne de la stratégie de SSI dans une entreprise, grâce à la sensibilisation.

> *« L'humain : dans un système sociotechnique, la composante humaine occupe une place particulière. Elle peut être source des plus grandes vulnérabilités mais également devenir un véritable rempart si les collaborateurs sont correctement sensibilisés et éduqués. C'est la partie auto apprenante du système. Ainsi, il est impératif de mettre l'accent sur le développement d'une culture de sécurité et de protection auprès des ressources humaines de l'entreprise. »*[19]

[19] HAPSIS. La protection de vos informations dans un environnement complexe [en ligne]. http://www.se-force.com/index.php?option=com_content&view=article&id=116&Itemid=152

5. Processus de sensibilisation

Maintenant que nous avons établi l'importance du facteur humain sur la SSI et les mesures de sécurité au niveau des ressources humaines qui peuvent être prises, nous allons regarder ce que des organismes, réputés dans le domaine des systèmes d'information, proposent comme processus pour réduire le risque humain sur le SI d'une entreprise. Nous regarderons ce qui est préconisé en matière de norme internationale concernant la sensibilisation des employés, puis nous analyserons ce que proposent des entreprises pour développer un programme de sensibilisation.

5.1 Norme

Dirigeons nous vers l'Organisation Internationale de Normalisation (ISO), premier producteur de normes au monde et sur laquelle beaucoup d'entreprises se basent pour harmoniser et améliorer, leurs activités. Ce sont des experts mondiaux qui établissent des normes dans différents domaines et les font ensuite ratifier par l'ISO. Ceux-ci définissent des exigences, des lignes directrices ou des caractéristiques à appliquer régulièrement pour assurer l'utilisation correcte des matériaux ou produits, ainsi que de l'optimisation des processus et services communs à tout organisme. (ISO, 2013)

C'est pour cette raison que nous allons regarder ce que l'ISO propose en termes de SSI au niveau des mesures de sécurité humaines.

5.1.1 Norme ISO 27002

L'organisation a créé une norme 27002:2005 qui établit un code de bonnes pratiques pour la gestion de la sécurité de l'information. Cette norme s'adresse à n'importe quel organisme pour la sécurité de son SI. Celui-ci n'est pas obligé de tout appliquer au pied de la lettre, il peut s'en inspirer pour mettre en place toute ou partie des recommandations faites dans cette norme. Ce document fait office de référence pour aider un organisme à établir ses objectifs de sécurité et mettre en place sa propre démarche de gestion de la sécurité. Il fait le tour de 133 mesures de sécurité à prendre en compte, pour aider les responsables dans le domaine de la sécurité, pour la mise en place d'un Système de Management de la Sécurité de l'Information (SMSI).

Politique de sécurité des systèmes d'information

En premier lieu, nous pouvons constater qu'elle propose d'établir un document qui est la *« Politique de sécurité des systèmes d'information »*[20] qui aide à la diffusion de la vision de l'entreprise en termes de sécurité, auprès de tous ses employés. En outre, établir une politique de sécurité des systèmes d'information est important pour permettre de passer en revue les risques qu'encourt le SI de l'entreprise, dans l'objectif d'installer différentes mesures techniques, organisationnelles, juridiques et humaines pour pallier à ceux-ci et éviter une catastrophe dont elle ne pourrait jamais se remettre.

Le CNRS explique :

> *« La politique de sécurité des systèmes d'information […] affiche un ensemble de principes d'ordre organisationnel [dont la formation et la sensibilisation au point 1.5 du même chapitre évoqué auparavant] et technique à caractère prioritaire. L'ensemble constitue un corps de doctrine pour la mise en œuvre de la SSI […] »*[21]

C'est le document de référence concernant la SSI au sein de l'entreprise. Il définit les objectifs à atteindre, les axes principaux à suivre et le règlement en matière de sécurité établi par l'entreprise, ainsi que les moyens accordés pour y parvenir. Celle-ci s'applique intégralement à toutes personnes autorisées à utiliser le SI de l'entreprise.

Il prend en compte la vision stratégique de l'entreprise et montre l'importance qu'accorde la direction à son système d'information. Il doit rester général, être mis à jour à intervalle régulier et utiliser un langage simple et compréhensible, afin que tous les utilisateurs du SI puissent le comprendre et mettre en pratique ce qui est proposé.

Enfin, il explique aux responsables chargé de la SSI que le règlement en matière de sécurité ne doit pas entraver l'utilisation quotidienne du SI pour éviter de contraindre les employés. Sinon l'effet inverse sera obtenu, ceux-ci le contourneront et ce n'est justement pas le but souhaité.

En d'autres termes, ce document a pour but de servir de guide les employés, mais aussi pour les responsables dans la mise en place d'un système de sécurité technique, organisationnel, juridique et humain au sein de l'entreprise.

---

20 Norme ISO 27002:2005 - Chapitre 5, p.6

21 ILLAND, Joseph pour le Centre national de la recherche scientifique. Politique de Sécurité des Systèmes d'Information [en ligne]. 1ère éd. Inconnu : CNRS, 2006. Page 17 http://www.dgdr.cnrs.fr/fsd/securite-systemes/documentations_pdf/securite_systemes/pssi-v1.pdf

Sécurité liée aux ressources humaines[22]

En deuxième lieu, cette norme propose un processus général de sensibilisation concernant un employé à son arrivée dans l'entreprise, durant son mandat et à son départ. Elle trace les lignes directrices pour la mise en place et la vérification d'une communication de sensibilisation dans une entreprise, auprès des employés en matière de sécurité de l'information. (Calé, Touitou, 2007)

> *« Dans le cadre de leurs obligations contractuelles, il convient que les salariés [...] se mettent d'accord sur les modalités du contrat d'embauche les liant et le signent. Il convient que ce contrat définisse les responsabilités de l'organisme et de l'autre partie quant à la sécurité de l'information. »*
>
> *(Norme ISO 27002:2005, p.24)*

Tout d'abord, la norme précise qu'il faut vérifier que le futur employé est à la hauteur des tâches potentiellement sensibles que l'entreprise aimerait lui confier. Ensuite, elle précise qu'il faut s'assurer que le candidat comprenne ses droits et ses devoirs face à la sécurité. Cela afin d'éviter un vol, une fraude ou un mauvais usage des ressources matérielles mises à disposition. Pour ce faire, il faut que l'entreprise établisse un contrat à signer concernant la description claire des tâches à effectuer, des droits, des devoirs et des responsabilités en matière de sécurité, dans l'entreprise.

> *« Il convient que l'ensemble des salariés d'un organisme […] suivent une formation adaptée sur la sensibilisation et reçoivent régulièrement les mises à jour des politiques et procédures de l'organisme, pertinentes pour leurs fonctions.»* *(Norme ISO 27002:2005, p.26)*

La norme indique qu'il faut vérifier durant toute la durée du contrat que les employés sont conscients des potentielles menaces sur le SI et des responsabilités qu'ils ont dans la sécurité des informations, ainsi que de respecter la politique de sécurité et des bonnes pratiques adoptées, afin de réduire le facteur de risque humain. Pour ce faire, la norme explique que l'entreprise doit faire bénéficier ses collaborateurs d'une formation pour les usages sécuritaires des ressources matérielles mises à disposition, ainsi qu'aux procédures et mesures de sécurité mise en place. Celle-ci doit se faire dès le départ, afin de réduire les menaces encourues sur le système d'information, et juridiques sur l'entreprise. De plus, l'entreprise doit présenter ses attentes vis-à-vis de son collaborateur, ainsi que les mesures et les politiques de sécurité mises en place. L'attention du collaborateur doit être attirée sur les responsabilités juridiques et les exigences en matière d'utilisation du système d'information. Elle préconise que cette formation soit adaptée à la fonction, au savoir-faire et aux responsabilités de l'employé. Enfin, il faut s'assurer qu'il comprenne et reconnaisse les menaces qui pèsent sur le SI

[22] Norme ISO 27002:2005 - Chapitre 8, p.22

et qu'il sache qui contacter en cas de suspicion. Nous verrons plus loin, que différents organismes proposent des méthodes de sensibilisation adéquates pour les collaborateurs.

L'entreprise peut aussi mettre en place un système de sanctions pour traiter les cas de violation du règlement.

> *« Il convient d'élaborer un processus disciplinaire formel pour les salariés ayant enfreint les règles de sécurité. […] Il convient que le processus disciplinaire formel garantisse un traitement correct et juste des salariés suspectés d'avoir enfreint les règles de sécurité »* *(Norme ISO 27002:2005, p.26)*

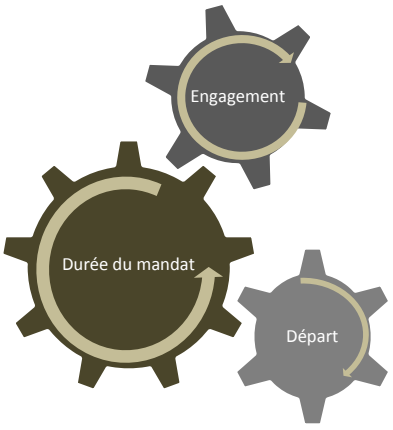
Ces mesures sont aussi mises en avant afin de prévenir un risque potentiel d'incident, cela permet d'augmenter l'attention portée à la sécurité de la part des employés. Evidemment, la norme tempère en expliquant que les sanctions doivent être proportionnelles à l'impact que l'incident a eu sur le SI et aux risques que celui-ci a fait courir à l'entreprise. Cependant, la norme dit que s'il est prouvé que l'incident a provoqué fait dans le but de nuire intentionnellement, il faut prendre les mesures nécessaires afin de rompre tout contrat liant les deux parties.

> *« Il convient que les responsabilités relatives aux fins ou aux modifications de contrats soient clairement définies et attribuées. »*
>
> *(Norme ISO 27002:2005, p.27)*

Enfin, pour garantir la sécurité des informations de l'entreprise lors de la fin d'un contrat, il faut vérifier que les ressources matérielles mises à disposition soient rendues en état et que les droits d'accès à l'intérieur du SI et de l'entreprise soient supprimés.

Nous pourrions résumer ces grandes lignes de sensibilisation, par le schéma ci-dessous :

Figure 12 : Processus de sensibilisation basée sur la norme ISO 27002:2005



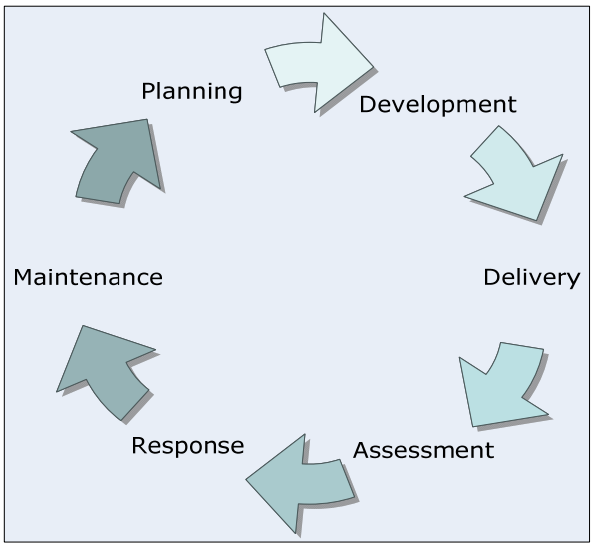
5.2 Méthodes

Nous avons donc compris que la norme ISO 27002:2005, propose d'établir une politique de sécurité afin de diffuser la vision de l'entreprise en matière de sécurité auprès de ses employés, ainsi qu'un processus de sensibilisation auprès d'eux depuis leur engagement à la fin de leur contrat en passant par une formation concrète durant leur mandat. Cependant, bien qu'elle donne des explications pertinentes et précises sur ce qui est attendu en entreprise au niveau de la sensibilisation, elle ne propose pas de processus exact quant à la communication et à la formation d'un employé. Alors, nous avons effectué d'autres recherches, afin de déterminer comment nous pourrions mettre en œuvre un processus concret de sensibilisation au sein d'une entreprise.

Après un grand nombre de recherches, nous avons constaté que beaucoup d'entreprises et organismes proposent des cours privés de sensibilisation pour les entreprises désireuses de former leurs employés. Mais peu proposent réellement de méthodes ou de guide libre d'accès en français.

Toutefois, nous avons trouvé deux grandes entreprises telles que Microsoft[23] ou l'ENISA[24] qui proposent des méthodes organisationnelles et des supports de communication libres d'accès à toutes les entreprises, souhaitant mettre en place par leurs propres moyens une campagne pour sensibiliser leurs utilisateurs.

Figure 13 : Cycle de vie d'un programme de sensibilisation selon Microsoft



(Microsoft, 2006, p.10)

[23] Microsoft. Facteurs clés pour le développement de programmes efficaces de sensibilisation et de formation à la sécurité des informations. In : Sensibilisation à la sécurité [en ligne]. 2006. http://technet.microsoft.com/fr-fr/security/cc165442.aspx

[24] ENISA. Le nouveau guide utilisateur : comment améliorer la sensibilisation à la sécurité de l'information. 2008, 110p. http://www.enisa.europa.eu/publications/archive/new-users-guide-fr

Figure 14 : Cycle de vie d'un programme de sensibilisation, selon l'ENISA

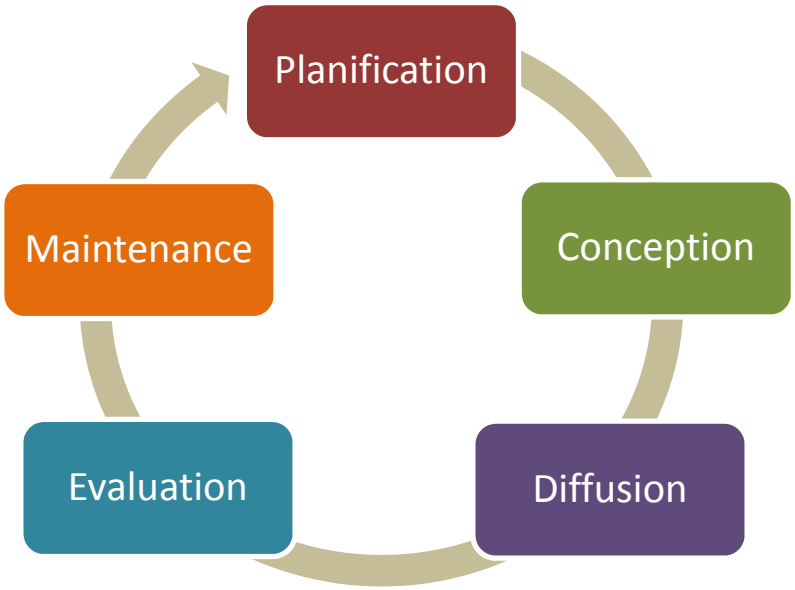
(ENISA, 2008, p.17)

Si nous nous basons sur ce que ces grands organismes proposent, nous pourrions faire ressortir cinq processus clés pour mener à bien une campagne de sensibilisation. Ces cinq processus sont les suivants :

- planifier ;
- concevoir ;
- diffuser ;
- évaluer ;
- maintenir.

Evidemment, chaque organisme propose des particularités qui leur sont propres. Néanmoins, nous pouvons en faire ressortir un fil rouge qui peut nous aider à mettre en place un programme de sensibilisation.

Figure 15 : Cycle de vie d'un programme de sensibilisation



5.2.1 Planification

Tout d'abord pour cette étape, les deux organismes sont d'accord pour dire qu'il est important qu'une planification de projet soit faite pour mener à bien un programme de sensibilisation. Ensuite, deux points leurs sont communs quant aux objectifs de la planification :

Constituer une équipe et déterminer les responsabilités de chacun

Ils précisent que pour ce genre de projet, il faut la participation et l'appui de plusieurs métiers appropriés, comme l'informatique, la communication et le marketing, les ressources humaines, le service juridique, la direction et les finances, dès le début du projet. L'ENISA précise qu'il faut choisir les collaborateurs qui ont le plus d'expérience dans le développement de projet, afin de mener à bien le programme.

Mais, surtout, il faut selon l'ENISA, le soutien de la direction, afin de montrer l'importance du projet et sa reconnaissance dans les plus hautes sphères de l'entreprise. Car, si les employés concernés ne voient pas l'importance du projet, ils ne soutiendront pas le programme et feront, selon l'ENISA de la « résistance passive »[25].

Evaluer le budget requis et l'obtenir

Toujours selon l'ENISA, *« Il est essentiel d'arriver à un consensus entre les décideurs concernant l'importance du programme et le bienfondé de son financement »*.Microsoft insiste sur le fait, qu'il faut allouer un budget totalement dévolu au projet, afin d'éviter que les dépenses se noient dans le budget global de la sécurité de l'entreprise. Toutefois, l'ENISA, nous met en garde *« […] envisagez et planifiez la possibilité que les fonds accordés soient insuffisants pour soutenir le programme de manière appropriée. »*[26]

[25] ENISA, 2008, p.29

[26] ENISA, 2008, p.22

5.2.2 Conception

Il s'agit de mettre sur pied un programme de sensibilisation. En ce qui concerne l'ENISA, certaines des recommandations ci-dessous sont présentes dans son processus de planification. Cependant, elle-même défini dans celui-ci deux autres points qui sont *« évaluer et concevoir »*[27]. Il nous est apparu plus judicieux de faire apparaitre les points qu'elle traitre à cette étape-ci, car évaluer et concevoir sont des points de développement spécifique pour le programme.

Il y a donc cinq points communs à cette étape pour ces deux organismes :

Définir les besoins et les objectifs

C'est pourquoi, L'ENISA et Microsoft propose tout d'abord de déterminer les besoins de sensibilisation réels des collaborateurs et les objectifs du programme, afin de pouvoir développer celui-ci en conséquence. Ils proposent tous les deux, dans leur méthode respective, une série de questions à se poser afin de cerner les points importants pour la détermination des ressources et du contenu à développer.

Déterminer les canaux de communication efficaces

Les deux organismes proposent ensuite, soit sur leur propre site, soit dans leur contenu des supports et des moyens de communication à utiliser pour sensibiliser les collaborateurs de l'entreprise.

Définir les groupes cibles

Pour cette étape, d'après l'ENISA, *« il est crucial de définir le public spécifique ciblé par l'initiative de sensibilisation. »*[28] Elle propose une série de question qui permet de pouvoir déterminé ces groupes. Quant à Microsoft, il n'en fait pas un point spécifique, mais parle souvent de groupe cible dans sa méthode, ce qui peut nous laisser penser qu'il est important pour lui aussi de déterminer qui bénéficiera de quel message et de quelle formation.

Elaborer le contenu de la communication des messages de sensibilisation et de la formation

A cette étape, il convient de traiter le contenu des informations et formation de sensibilisation, déterminer les messages pertinents et les supports adéquats pour transmettre un savoir-faire aux collaborateurs. Chaque organisme a sa vision de la communication. L'ENISA propose de suivre des règles de base pour rester pertinents

[27] ENISA, 2008, p.16

[28] ENISA, 2008, p.22

et efficaces, alors que Microsoft explique qu'il faut prendre en compte des mécanismes de diffusion spécifiques afin que la communication soit efficace.

Prévoir des ressources pour évaluer l'efficacité du programme

Afin de définir l'efficacité du programme proposé tant avant sa mise en route qu'après la fin de sa session, tous deux proposent de développer des ressources.

> *« Evaluer une campagne ou un programme est essentiel pour appréhender son efficacité ainsi que pour utiliser les données comme indications pour corriger l'initiative afin de la rendre encore plus fructueuse. »* *(ENISA, 2008, p.54)*
>
> *« […] Il est nécessaire de développer un moyen efficace permettant de rapporter […] aux cadres de direction les informations glanées au cours du processus mesurant la compréhension et la satisfaction à l'issue de la session de formation »* *(Microsoft, 2006, p.19)*

Microsoft propose, en plus, de mettre en place avant la diffusion à grande échelle, un programme pilote sur un petit groupe de collaborateurs afin d'évaluer la pertinence, et l'efficacité, ainsi que d'améliorer les éventuels défauts du programme. Tandis que l'ENISA propose de mettre en place des indicateurs chiffrables et de préparer des questionnaires à faire circuler, après les sessions de sensibilisation, auprès des collaborateurs participants.

5.2.3 Diffusion

A cette étape, les deux organismes s'accordent pour dire que *« Lorsqu'un plan bien écrit est mis en place et que vous disposez aussi des ressources appropriées pour l'exécuter, le moment est venu de demander aux différents acteurs choisis au préalable pour créer le programme et l'exécuter en vue de concrétiser les avantages de la sensibilisation à la sécurité de l'information. »* *(ENISA, 2008, p.67)*

De plus, tous deux précisent qu'il ne faut pas oublier de récolter les impressions et les suggestions des collaborateurs participants, afin de pouvoir intégrer leurs remarques au processus de mise à jour du programme.

5.2.4 Evaluation

L'évaluation doit être faite après chaque session de sensibilisation et de formation des employés. L'ENISA précise que cette étape est un point à ne pas omettre, car il s'agit d'évaluer les informations générées par le programme, de déterminer si les objectifs principaux ont été atteints et d'ajuster les processus de travail avec les différentes informations reçues. De plus, Microsoft précise que l'évaluation permet de rendre compte, si les collaborateurs ont bien compris les messages diffusés, et qu'ils ont bien été impliqués dans le processus de formation. Cette étape a donc pour objectif de recevoir des indications sur l'efficacité de la campagne diffusée au préalable.

5.2.5 Maintenance

A cette étape, il est bien expliqué par Microsoft, que le programme ne s'arrête pas après sa première exécution.

> *« Les programmes ne prennent pas fin une fois le premier cycle de sessions achevé avec succès. Ces programmes représentent un investissement constant dans lequel votre organisation doit s'engager. »* *(Microsoft, 2006, p.23)*

L'ENISA propose d'intégrer les enseignements tirés de l'évaluation afin de l'intégrer au processus de mise à jour.

> *« Les expériences accumulées depuis le lancement du programme fournissent les connaissances et la compréhension nécessaires pour rectifier le programme en vue de sa réussite. »* *(ENISA, 2008, p.76)*

Il faut constamment le tenir à jour car les menaces, la technologie, ainsi que les exigences juridiques évoluent avec le temps. De plus, selon Microsoft, les équipes du projet, les mesures organisationnelles et techniques, ainsi que les règlements peuvent aussi changer. Microsoft insiste encore sur le fait qu'il faut maintenir le programme sur le long terme, car c'est la meilleure façon de sensibiliser les collaborateurs.

5.3 Comment adapter la communication

Après avoir déterminé les moments où il faut sensibiliser les utilisateurs via la norme 27002, et par quelles étapes un plan de sensibilisation se construit comme établit au point précédent, il faut maintenant s'intéresser à l'aspect communicationnel. Nous avons vu au chapitre précédent que des professionnels en sécurité des systèmes d'information ont établi qu'il y avait une nouvelle génération « *connectée* »[29] grandissante au sein des entreprises et que, par conséquent, il faut adapter la manière de sensibiliser ces utilisateurs. Pour cela, les auteurs du livre blanc *« Sensibilisation à la sécurité de l'information 2.0 »*[30] donnent des conseils pour rendre la communication faite aux utilisateurs plus attractive.

5.3.1 Convaincre, communiquer et impliquer

Tout d'abord, les auteurs de ce livre explique qu'il faut persuader les collaborateurs, en leur démontrant par des exemples que cela n'arrivent pas qu'aux autres. *« [..]Il est essentiel d'expliquer, de démontrer, de donner des exemples… »* Cette génération est ultra connectées, elle est au courant de tout, tout le temps, donc il faut utiliser ce chemin pour les informer de manière continue quotidiennement. *« Il sont habitués à recevoir des informations en permanence avec les médias, les réseaux sociaux, et l'Internet. »*

Ils prendront conscience de l'importance de la sécurité et que l'entreprise compte sur eux. *« La sécurité d'une entreprise dépend bien de chacun de ses employés. »* En plus, ils se sentiront impliqués dans le processus de sécurité et seront ravis de pouvoir contribuer à la sécurité de l'information de leur entreprise.

5.3.2 Message court et original

Ensuite, ils proposent de trouver un original moyen pour communiquer les attentes de l'entreprise en matière de sécurité, de manière courte et simple. *« Il faut les accrocher et aller rapidement à l'essentiel […] la clé du succès est de surprendre et d'intriguer les interlocuteurs. Il est essentiel de faire preuve d'originalité […] »*

---

[29] BENNASAR, Matthieu, BRIGAUD, Julien, COMBES, Létitia. *Sensibilisation à la sécurité de l'information 2.0* [en ligne]. Livre Blanc. PARIS : LEXSI – INNOVATIVE SECURTIY, 2013. Pages 7-8 https://www.lexsi.fr/sites/default/files/publications/lb_sensibilisation_a_la_securite_de_linformation_2.0.pdf

[30] Les citations inclus dans ce chapitre qui proviennent de ce livre blanc sont toute à la page 6.

5.3.3 Moyen interactif

Après, selon les auteurs, il s'agit de trouver un novateur moyen et adapté à leur génération pour les faire participer de manière interactive et amusante, ainsi ils seront ravis de collaborer. *« Un utilisateur [de cette génération] ne retient que s'il participe… […] Apprendre en s'amusant est un des moyens de les toucher directement et de les faire s'intéresser à la sécurité. »* Ainsi, ils retiendront ce qu'ils ont appris, parce qu'ils auront été impliqués dans le processus, et ils s'intéresseront d'avantage à la sécurité.

5.3.4 Tester les connaissances

Enfin, comme nous l'avons vu auparavant, ces utilisateurs connaissent très bien les technologies, et d'après les auteurs, ils pensent déjà tout connaitre. *« Il faut aller plus loin en les testant grandeur nature, pour mettre en évidence leurs limites et remettre en cause leur confiance en eux. »* C'est en testant leurs connaissances, selon les auteurs, que les responsables de la sécurité provoqueront chez eux une réflexion sur leurs réelles connaissances et ainsi ils apprendront de leurs erreurs.

5.4 Les canaux de communication

Pour finir, pour mettre en place une bonne culture de la sécurité de l'information au sein d'une entreprise, il faut travailler sur les trois dimensions que représente la sensibilisation, qui sont, pour rappel, l'information, la communication et la formation. Ainsi, il est judicieux de déterminer les canaux de communication adéquats pour véhiculer les informations relatives au programme de sensibilisation voulu au sein d'une entreprise. Pour ce faire, nous trouvons beaucoup de conseils sur internet, avec différents points à aborder ou encore des moyens de communication et de formation, qui se ressemblent tous, au final.

Le CERN, par exemple, propose des cours privés, mais aussi différents supports d'exemples, afin de mener à bien une communication sur la sécurité informatique dans les entreprises. L'EPFL et le CASES aussi propose des supports de communication. L'ENISA fournit une multitude de supports à disposition de tous sur son site internet. Dans son guide utilisateur, elle indique quelques canaux de communication intéressants à mettre en place, ainsi que leurs avantages et leurs inconvénients. Tout comme, dans le livre blanc *« Sensibilisation à la sécurité de l'information 2.0 »*[31]. Microsoft propose aussi des masques pour des supports de communication adéquats, comme expliqué auparavant. Enfin, dans les nombreux livres que nous avons lu, ce trouve quelques conseils et exemple pour rédiger une politique de sécurité, ainsi qu'une charte utilisateur à l'attention de ses collaborateurs.

Vous trouverez en annexe 1 la liste des différents canaux de communication intéressants et proposés par ces différents organismes, avec leurs avantages et leurs inconvénients. Nous les avons triés selon les trois dimensions de sensibilisation que nous avons vues précédemment, ainsi nous pouvons mieux cerner le contexte dans lequel ils peuvent être utilisés par une équipe chargé de mettre en place un programme de sensibilisation.

[31] BENNASAR, Matthieu, BRIGAUD, Julien, COMBES, Létitia. *Sensibilisation à la sécurité de l'information 2.0* [en ligne]. Livre Blanc. PARIS : LEXSI – INNOVATIVE SECURTIY, 2013. Pages 9-10 https://www.lexsi.fr/sites/default/files/publications/lb_sensibilisation_a_la_securite_de_linformation_2.0.pdf

5.5 Solution informatique

Enfin, durant nos recherches, nous avons constaté qu'il existe une solution informatique pour gérer entièrement une campagne de sensibilisation à la sécurité du système d'information. Nous avons donc pris contact avec les deux entreprises[32] trouvées qui proposent cet outil afin de les essayer durant une trentaine de jours comme proposé. Seule une entreprise a répondu[33], cependant, elle n'était pas en mesure de nous fournir l'application de démonstration, car notre travail n'avait pas de fins professionnelles. Néanmoins, nous pouvons quand même supposer, selon la description qui en est faite, qu'une solution informatique comme celle-là permet de faciliter la gestion complète d'un programme de sensibilisation, étant donné que toutes les différentes phases abordées dans ce chapitre s'y trouvent.

5.6 Conclusion

En conclusion, d'après tous ces organismes et entreprises experts dans le domaine de la sécurité des systèmes d'information, il est important :

- D'établir une politique de sécurité des systèmes d'information qui reflète la vision stratégique de l'entreprise et précise la ligne générale à suivre en matière de sécurité du système d'information. Dans le but de diffuser la culture en matière de sécurité de l'information auprès des collaborateurs.

- De commencer la sensibilisation d'un employé dès son engagement jusqu'à son départ. Et de développer un programme de sensibilisation qui soit le plus adapté possible aux utilisateurs du SI afin de les intéressés, et de les joindre au processus de sécurité, afin d'en faire les acteurs principaux pour la protection de l'information au sein de l'entreprise.

Ainsi ces deux points cruciaux permettront en interne d'homogénéiser les bonnes pratiques sécuritaires et de diffuser une culture de la sécurité commune à tous à travers l'entreprise et en externe de renvoyer une image et une réputation responsable et professionnelle à ces partenaires commerciaux.

---

[32] Conscio-technologies. Sensiwave, un nouveau lien entre l'entreprise et ces collaborateurs [en ligne]. http://www.conscio-technologies.com/?option=com_content&view=article&id=109&Itemid=92

Terranova. Sensibilisation Sécurité de l'Information [en ligne]. http://www.tnawareness.com/fr/securite-information

[33] Voir la réponse à notre demande à l'annexe 2.

6. Dans la réalité

Pour tenter de comprendre réellement comment les entreprises sensibilisent et forment, sur le terrain, leurs employés à la sécurité des systèmes d'information, nous nous sommes rendus dans trois entreprises du domaine tertiaire, représentants des activités différentes, ainsi que dans deux Hautes Ecoles Spécialisées.

6.1 Interviews - secteur privé[34]

Pour ce faire nous avons interrogé un collaborateur de chaque, qui travaille dans le département informatique interne à l'entreprise. Nous avons été dans une banque, une multinationale et une moyenne entreprise (PME) basée à Genève.

Nos questions se portent sur la politique de sécurité établie au sein de l'entreprise concernant les employés et sur la sensibilisation de la sécurité des informations à l'intérieur de l'entreprise. Nous souhaitons comprendre sur quelles bases ils créent leur politique de sécurité, de quelle manière ils sensibilisent leurs collaborateurs et comment ils diffusent ces bonnes pratiques auprès des employés. En outre, nous leur avons demandé si leurs collaborateurs mettent en œuvre ces bonnes pratiques et s'ils pouvaient émettre une hypothèse qui expliquerait pourquoi ceux-ci les appliquent-ils ou non. Enfin, nous leur avons demandé si leur politique en matière de sensibilisation fonctionnait selon leurs attentes.

6.1.1 Banque

Au sein d'une banque la sécurité est essentielle tant au niveau des infrastructures électroniques et informatiques, qu'au niveau humain. La réputation de l'entreprise tient entre autres sur deux bases essentielles qui sont la confidentialité et la sécurité des informations avec lesquelles elle travaille. Sans une politique de sécurité et une culture d'entreprise qui mise sur la discrétion, la réputation de la banque en pâtit.

C'est pourquoi, nous avons interviewé un collaborateur d'une banque de Genève, travaillant au sein du support informatique de l'entreprise, afin de comprendre comment celle-ci agit pour limiter le facteur de risque humain sur le système d'information.

Vision de la sécurité transmise dès le début

Leur politique de sécurité est communiquée à l'engagement de chaque employé, ainsi que lors d'une réunion de présentation de l'entreprise. Les règles sont très strictes, en

[34] Vous trouverez les interviews des entreprises à l'annexe 3

matière de sécurité. Rien ne sort, ni ne rentre quel que soit le support de stockage. De plus, chaque nouvel employé reçoit une petite formation à son arrivée.

Politique de sécurité accessible

Cette politique est accessible sur l'intranet de l'entreprise, et cette information est communiquée aux employés, ainsi s'ils estiment en avoir besoin, ils savent où la trouver pour la consulter. Cependant, notre interlocuteur explique qu'il n'est pas sûr que chaque employé se souvienne où il peut la trouver. Elle est basée sur les normes de sécurité en vigueur, l'expérience de la banque et de ses responsables informatiques, ainsi que sur l'actualité. Elle est mise à jour selon le même principe que son établissement, au gré de l'actualité, des audits internes, de l'évolution des normes de sécurité et de la technologie.

Equipe chargée de la sécurité

Au sein de la banque, c'est une équipe spécialement chargée de la sécurité de l'information qui édicte les règles de sécurité. Selon notre interlocuteur, il y a une distinction qui est faite selon les domaines métiers et les niveaux hiérarchiques à l'établissement de cette politique, afin d'accroitre la sécurité et d'adaptée ces règles au contexte de travail. Ces règles de sécurité sont extrêmement bien expliquées aux employés, afin qu'ils comprennent leur importance.

Mesures techniques appuient les mesures organisationnelles

Afin qu'elles soient appliquées correctement au quotidien, les administrateurs systèmes utilisent les outils informatiques pour restreindre un maximum les éventuels mauvaises manipulations. Ainsi, ils évitent de laisser toute la responsabilité de la sécurité des informations aux employés, grâce au à l'infrastructure du système informatique mis en place, ils peuvent d'une certaine manière diriger les employés dans une manipulation sécurisée et réfléchie des outils et autres gestes utiles dans leur travail.

Conscients et informés, mais pas forcément attentifs

Actuellement, notre interlocuteur ne pense pas que les utilisateurs au sein de l'entreprise soient réellement conscients de l'importance des informations qu'ils manipulent chaque jour. En effet, vu la quantité traitée quotidiennement, ils peuvent rapidement ne plus faire attention à ce qu'ils font, car il s'agit d'être performant dans leur travail. Il estime tout de même que si les utilisateurs sont attentifs, c'est par conscience professionnelle. Mais aussi et souvent par obligation, et se sentent parfois contraints. Il nous explique que la sensibilisation à la sécurité des informations, mise

en place auprès des employés, a été testée. Malheureusement, il s'avère qu'il y a peu d'employés qui appliquent toutes les règles de sécurité.

Mesures organisationnelles bonnes dans l'ensemble

Quand nous lui demandons s'il juge suffisant les mesures mises en place afin de restreindre le risque humain, il nous explique qu'il y a toujours un potentiel d'amélioration, mais il y a aussi une question de coûts et cela entre tout de même en compte dans la politique générale de sécurité.

En conclusion, dans ce cas-là les outils électroniques et informatiques sont actuellement un bon moyen de palier au risque humain des employés respectueux de l'entreprise. Ces outils agissent comme un filet de sécurité pour rattraper les éventuelles erreurs commises inconsciemment par les employés pris par leurs tâches et responsabilités quotidiennes. Mais il y aura toujours un risque venant d'un employé mal intentionné qui pourra contourner le système afin de nuire à l'entreprise. Pour ceux-là, la seule sanction est la mise à la porte immédiate. Pour les autres d'après notre interlocuteur, le cas est évalué.

6.1.2 Multinationale

Voyons maintenant comment cela se passe dans une entreprise multinationale, dont un de ses objectifs de sécurité de protéger ses données, ainsi que d'éventuelles nuisances pour ses affaires.

Nous avons donc interrogé un collaborateur travaillant au sein du support informatique de l'entreprise, qui a pu nous éclairer quant à la politique générale de sécurité et la communication qui a été mise en place.

Vision de la sécurité transmise dès le début

Leur politique de sécurité est communiquée à l'engagement d'un nouvel employé, et lors de la réunion rassemblant les nouveaux collaborateurs pour la présentation de l'entreprise. Les responsables de la réunion prennent le temps d'expliquer l'importance de ces règles de sécurité et les bonnes pratiques qu'il faut mettre en œuvre lors de l'usage des outils informatiques de l'entreprise. Afin de bien faire passer le message, ils utilisent des exemples d'ingénierie sociale* pour marquer les esprits.

Politique de sécurité accessible

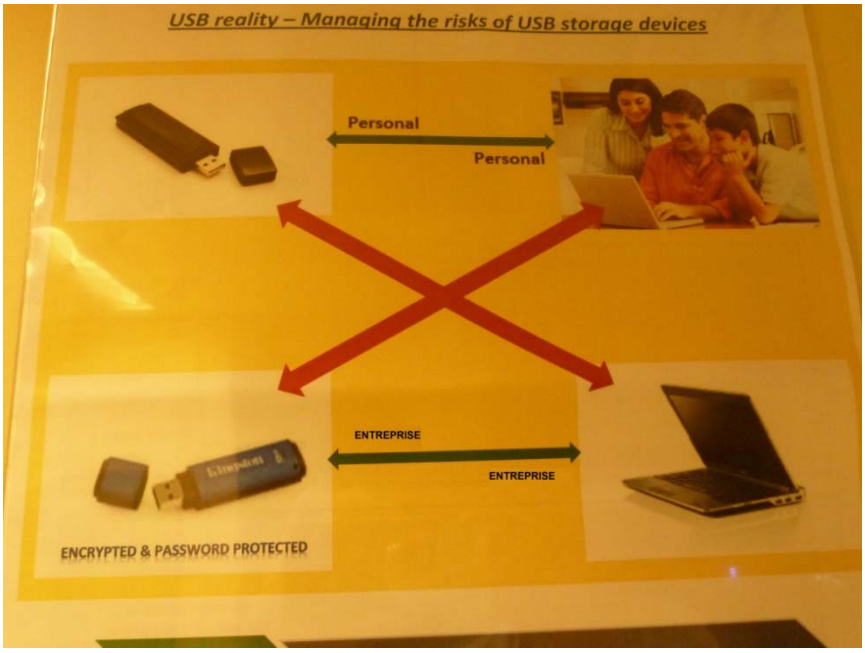
Cette politique de sécurité est disponible sur l'intranet de l'entreprise. Cependant, notre interlocuteur n'était pas sûr de savoir où la trouver, afin de pouvoir nous la montrer.

Pourtant, notre interlocuteur s'est dirigé instinctivement sur l'intranet de l'entreprise pour voir s'il pouvait y avoir accès. Il n'est donc pas sûr que chaque employé se souvienne où il peut la trouver. Cette politique de sécurité évolue selon les besoins de l'entreprise, ainsi qu'au gré des audits internes effectués par une entreprise externe, suivant les normes de sécurité en vigueur. Ces règles sont communes à tous les collaborateurs, néanmoins, il pense qu'il y a peut-être une ou deux exceptions selon le travail effectué au sein de la compagnie.

Equipe chargée de la sécurité

L'équipe se charge d'établir ces règles sur la base des normes de sécurité en vigueur, de l'expérience des responsables des technologies de l'information et de l'historique de l'entreprise, ainsi que sur l'actualité. Cette équipe diffuse ces règles de bonnes pratiques ou ces avertissements de sécurité de manière écrite et orale, quelques fois par année par mail, ou sur des posters accrochés aux murs des lieux communs à chaque étage. De plus, elle organise deux fois par année des séances d'information facultatives axées sur un sujet en particulier, ouverte à tous les collaborateurs pour qu'ils puissent poser leurs questions.

Figure 16 : Exemple d'affiches dans les lieux communs de l'entreprise[35]



(Entreprise multinationale, 2013)

[35] Photo prise dans l'entreprise le jour de l'interview le 30 juillet 2013.

Compromis entre mesures techniques et activités professionnelles

Bien que les collaborateurs de l'entreprise soient informés des mesures de sécurité à adopter au quotidien, les employés ne comprennent pas toujours l'importance de l'enjeu qui est derrière ces bonnes pratiques.

En effet, ils souhaitent avoir un outil accessible facilement et rapidement, afin de travailler sans contrainte au détriment des mesures de sécurité demandées par l'entreprise. C'est pourquoi, l'équipe de gouvernance de la sécurité, ainsi que celle du service informatique essayent de trouver une juste mesure dans les contraintes imposées aux collaborateurs. Ils évaluent les risques réels qui peuvent survenir pour éviter d'être trop extrême dans leurs décisions et ainsi nuire aux affaires. Ils mettent, donc, en place le minimum d'infrastructure pour répondre aux besoins de sécurité et comptent aussi sur la responsabilité des utilisateurs pour éviter d'éventuels incidents. C'est une sorte de compromis.

Conscients et informés, mais pas forcément attentifs

Pour le centre informatique, si une majorité d'utilisateurs appliquent ces bonnes pratiques, c'est par conscience professionnelle, bien qu'ils se sentent contraints, ils savent que c'est important pour l'entreprise, et que cela peut avoir un impact considérable sur leur travail et les affaires de celle-ci. Malheureusement, pour la petite minorité des utilisateurs qui ne mettent pas souvent en œuvre ces bonnes pratiques, c'est dû la plus part du temps à un oubli de leur part, et non un problème d'inconscience.

Si un incident venait à être signalé, une équipe interne s'occupe de rechercher toutes les traces laissées dans le système, afin de connaitre le responsable et les dégâts commis. Ensuite des mesures sont prises selon la gravité et la fréquence des mauvaises manipulations.

Soutient de la part de la direction

La direction de cette entreprise a bien compris que le risque humain existait, et c'est pour cette raison que même lors d'un remaniement budgétaire, l'équipe de gouvernance de la sécurité n'est pas impactée par une décision d'argent.

Notre interlocuteur estime tout de même que la sensibilisation faite auprès des utilisateurs est bonne, bien que des améliorations puissent être faites.

En conclusion, dans cette entreprise, les mesures de sécurité ont été jugées selon l'impact qu'elles pouvaient avoir sur les affaires de l'entreprise. Elles sont évaluées de manière à prendre en compte le risque réel qui pourrait survenir et ainsi éviter aux

collaborateurs des manipulations qui pourraient les amener à contourner le système, afin de faire leur travail plus rapidement. L'entreprise utilise même des supports de communication adaptés aux employés. Comme les posters qui expliquent ce qu'ils doivent faire ou non selon une situation, et ceux-ci sont mis dans les lieux communs là où ils peuvent prendre le temps de les lire.

6.1.3 PME

Pour finir, nous avons interviewé le directeur du service informatique d'une moyenne entreprise de Genève, afin de comprendre comment elle aussi communique et diffuse sa politique de sécurité auprès de ses collaborateurs pour limiter les incidents de type humain sur son système d'information.

Vision de la sécurité transmise dès le début et politique de sécurité accessible

Leur politique de sécurité est, comme les deux autres entreprises, communiquée à l'engagement d'un nouvel employé. Cependant, un mail lui est envoyé dès l'activation de sa messagerie, lui expliquant qu'il peut la trouver en première page de l'intranet de la compagnie, ce qui change des deux premières entreprises.

Equipe chargée de la sécurité

L'équipe informatique, le responsable de la sécurité et la direction de l'entreprise se chargent d'établir ces règles sur la base des normes de sécurité en vigueur, l'expérience de l'équipe, l'historique de l'entreprise, ainsi que sur l'actualité et les informations communiquées lors de conférences.

Cette équipe diffuse ces règles de bonnes pratiques ou ces avertissements de sécurité de manière écrite et orale. La politique de sécurité évolue constamment selon les besoins de l'entreprise. Elle envoie donc un mail dès qu'il y a un changement. De plus, en matière de sensibilisation, elle informe ses collaborateurs par courrier électronique avec des exemples réels à l'appui pour mieux faire comprendre l'importance de ces règles de sécurité. Elle envoie aussi des courriers électroniques de rappels tous les deux mois.

Formation des employés

De plus, elle propose des séances de formation continue pour sensibiliser ses employés, ce que ne font pas les deux autres entreprises. En outre, il y a des distinctions au niveau des métiers de l'entreprise concernant les informations, la sensibilisation et la formation donnée aux employés. En effet, les techniciens qui installent des applications ou des infrastructures informatiques dans d'autres

entreprises, nécessitent une formation régulière et plus rigoureuse sur la sécurité qu'un employé interne.

Conscients et informés, mais pas forcément assidus

Cependant, notre interlocuteur n'est pas sûr que tous les employés comprennent l'importance de ces règles. Parfois, certains d'entre eux pensent que c'est exagéré. Selon lui, si certains employés sont conscients des enjeux de la sécurité, d'autres les appliquent par contrainte ou encore parce qu'ils doivent le faire sans forcément toutes les comprendre.

L'équipe informatique a mis en place un certain nombre de mesures techniques, afin de limiter les manipulations qui pourraient avoir des conséquences pour l'entreprise. Cependant, elle fait aussi confiance aux les utilisateurs et compte sur eux pour qu'ils soient vigilants. Notre interlocuteur estime qu'il ne pourrait surement pas faire mieux en termes de mesures de sensibilisation, qu'elles sont suffisantes pour le moment.

L'entreprise a les moyens de savoir si un employé a enfreint les mesures de sécurité mises en place. Si un incident venait à être détecté, des mesures proportionnelles à l'importance de l'incident sont prises à l'encontre de l'employé.

Soutient de la part de la direction

La direction de cette entreprise a bien compris l'importance de la sensibilisation des employés à la sécurité informations professionnelles, puisqu'elle prend, d'ailleurs, part à l'élaboration de la politique de sécurité. Il est donc aisé, selon notre interlocuteur, de négocier un budget, mais pas directement pour la sensibilisation, cela fait partie d'un tout. En outre, il n'y a jamais eu de restriction budgétaire pour la sécurité, ce qui montre que la sécurité a une grande importance dans cette entreprise.

Pour finir, notre interlocuteur estime que la sensibilisation faite dans l'entreprise, auprès des utilisateurs est bonne. D'ailleurs, il s'en aperçoit lorsque ceux-ci font attention et posent des questions.

En conclusion, la sensibilisation des employés est prise très au sérieux par les instances dirigeantes. La politique de sécurité est mise en avant sur l'intranet de la compagnie, et un mail indique au nouvel employé où il la trouver en cas d'interrogation de sa part. De plus, la campagne de sensibilisation qui a été mise en place dans cette entreprise, passe par les trois dimensions vues précédemment et elle s'adapte aux besoins de chaque métier de l'entité. Les responsables utilisent judicieusement des exemples réels, afin de démontrer l'importance des messages de sécurité qu'ils souhaitent faire passer. Enfin, nous pouvons voir que les employés s'interrogent sur la

sécurité et n'hésitent pas à poser des questions auprès du centre informatique, ce qui montre que la sensibilisation établie porte ses fruits.

6.1.4 Impacts de la sensibilisation dans le secteur privé

Nous pouvons retenir ici, que les entreprises interviewées rendent attentif leurs nouveaux collaborateurs à la politique de sécurité en vigueur à l'intérieur de l'infrastructure dès leur arrivée, soit lors de la discussion des conditions d'emploi, soit de manière plus générale lors d'une présentation de l'entreprise. Nous remarquons aussi que chacune explique à tous ses collaborateurs l'importance de ces règles et comment les appliquer. Elles ont toutes mis à disposition leur politique de sécurité sur l'intranet, support accessible à tous les employés. Deux des entreprises sondées proposent une formation ou une séance d'information durant le mandat afin que les employés puissent en apprendre plus. Une seule entreprise cependant envoie un courrier électronique à ses nouveaux collaborateurs pour leur expliquer où ils peuvent retrouver la politique de sécurité, si besoin. Néanmoins, une autre a décidé de faire une campagne d'explication et de sensibilisation continue à travers des affiches avec des mots et des images simples pour faire passer rapidement un message de sécurité auprès de ses collaborateurs. Toutefois, chacune d'entre elles diffusent un rappel des mesures en vigueur ou des nouveautés en matière de sécurité tous les trois mois en moyenne. De plus, chacune ont une équipe dédiée à la sécurité des systèmes d'information.

En conclusion, chaque entreprise interrogée est consciente des risques qui découlent de leurs propres employés et mettent en œuvre une politique de sécurité au sein de l'entreprise qui permet de sensibiliser sur au moins deux des trois dimensions, vues précédemment, chaque collaborateur dès son arrivée, durant son mandat et jusqu'à son départ. De plus, la manière dont elles diffusent leurs explications fonctionne, puisque chaque interlocuteur estime que le résultat est concluant.

6.2 Interviews - Hautes Ecoles Spécialisées

Comme notre travail est principalement axé sur deux Hautes Ecoles Spécialisées précises qui sont la Haute Ecole de Santé (HEDS) et la Haute Ecole de Gestion (HEG) de Genève. Nous avons interviewé une vingtaine de collaborateurs, dont les utilisateurs du système d'information, ainsi qu'un membre de la direction et du service informatique de chacune d'elle. Dans le but de comprendre comment est mise en place la sensibilisation au sein de ces deux écoles.

Tout d'abord, expliquons rapidement, quel est le but d'une Haute Ecole Spécialisée (HES). C'est une université de type professionnelle, qui *« […] dispense un enseignement de niveau tertiaire, axé sur la pratique, dans le prolongement d'une formation post-obligatoire professionnelle. »*[36]

Elle réalise en plus de l'enseignement, des projets de recherches dont les résultats servent à améliorer l'enseignement dispensé, fournit des prestations à des tiers et assure un échange avec le milieu professionnel. Ces objectifs lui confèrent une réputation importante au niveau Suisse. Ce type d'école joue un rôle important au niveau de la formation nationale, elle délivre des diplômes formateurs, qui sont reconnus au niveau national et international. Elle collabore aussi avec d'autres entités de formation et de recherches à travers le monde.

6.2.1 Haute Ecole de Santé[37]

Cette Haute Ecole forme des professionnels de la santé. Ce domaine nécessite une confidentialité accrue sur les dossiers des patients, ainsi que le secret professionnel sur les traitements administrés.

Communication de base

Après avoir interviewé six personnes au sein du corps administratif et enseignant, nous avons pu constater qu'une sensibilisation basique à l'utilisation sécurisée des outils informatiques, a été diffusée oralement par le centre informatique.

[36] HAUTE ECOLE SPECIALISEE DE SUISSE OCCIDENTALE. Qui sommes-nous [en ligne]. http://www.hes-so.ch/fr/sommes-nous-26.html

[37] Vous trouverez les interviews des collaborateurs de la HEDS à l'annexe 4

En effet, lorsqu'un employé prend ces fonctions au sein de l'école, un administrateur système communique ces trois règles de base :

- Verrouiller le poste de travail lorsqu'il quitte sa place ;
- Enregistrer ses documents sur son espace de profil personnel et non sur son bureau, afin d'éviter la perte de ses fichiers si une panne devait survenir ;
- Les clés USB sont fragiles, et doivent être enlevée du poste correctement.

Ces règles sont communiquées, selon lui, pour de rendre attentif les utilisateurs à l'utilisation correcte d'un ordinateur.

Prise de mesures personnelles

Cinq des collaborateurs interrogés prennent des mesures en plus de celles communiquées pour mieux sécuriser l'information, car leurs postes les y obligent. Cependant, le dernier collaborateur ne se souvient pas avoir été sensibilisé à de quelconques manipulations de sécurité avec son ordinateur à son engagement et il aurait aimé pouvoir les trouvées sur l'intranet de l'école.

Toutefois, le responsable informatique explique que seule la charte est disponible sur l'intranet, et que les explications données, à l'engagement d'un collaborateur, ne le sont pas.

Campagne de sensibilisation datée

Concernant la charte informatique disponible sur l'intranet Qualité de la Haute Ecole Spécialisée de Genève (HES-Genève), deux employés, engagés il y a deux ans, ne savaient pas que cela existait et qu'elle était disponible à cet endroit. Néanmoins, pour les quatre autres collaborateurs travaillant depuis plus de 10 ans au sein de l'école, ils s'en souviennent vaguement.

En effet, il s'avère qu'en 2005, l'ancien directeur adjoint de l'école et l'actuel responsable informatique, ont établi une charte informatique et une communication concernant les règles de sécurité qu'ils ont présenté lors d'une séance plénière à tous leurs collaborateurs. De plus, ces employés se souviennent, dans la continuité de cette sensibilisation, avoir reçu des rappels ou des avertissements concernant de potentiels risques durant les deux années suivantes. Le responsable informatique, qui est en place depuis plus de 12 ans, confirme effectivement cette approche de la sensibilisation mise en œuvre.

Information perdue dans la masse

Depuis, cependant, plus rien n'a été fait, d'après les utilisateurs, pour poursuivre cette sensibilisation à la sécurité du système d'information.

Le responsable informatique, cependant, nous explique qu'il est très rare qu'il émette des avertissements, car il n'y a pas eu de menaces depuis. Mais il rappelle certaines informations au moins une fois par année par courrier électronique ou oralement.

Ces collaborateurs ne se souviennent pas avoir lues ces informations, mais supposent tout de même qu'elles soient passées inaperçues dans la masse de courriers électroniques reçues à la rentrée.

Vision des utilisateurs face aux mesures de sécurité conseillées

Tous les collaborateurs interviewés comprennent très bien pour qu'elle raison ils doivent faire attention, chacun les applique dans la mesure de ses connaissances et par conscience professionnelle. Il n'y a donc pas de problème de ce côté-là. Cependant, ils estiment qu'ils manquent d'explications sur les mesures à prendre ou les manipulations à ne pas faire sur un ordinateur. Ils pensent que le service informatique a négligé ce point dans leur politique de sécurité ou qu'ils ne sont pas assez exhaustifs.

Vision du service informatique face aux mesures de sécurité appliquées

Selon le responsable, il y a les collaborateurs qui comprennent et mettent en place les informations, et ceux qui laisse courir jusqu'au jour il leur arrive quelque chose. En outre, il estime que la manipulation d'un ordinateur requiert des compétences en bureautique et que chacun devrait les avoirs acquis depuis le temps. Cependant, il estime tout de même que ces informations ne sont pas suffisantes.

Contraintes et temps ne joue pas en faveur de la sécurité

D'après le responsable informatique, des mesures techniques de sécurité plus fortes avaient été mises en place un temps, mais les utilisateurs les trouvaient qu'elles étaient trop contraignantes, c'est pourquoi il a réduit les mesures. Mais il déplore un manque de temps pour pouvoir réellement tester si les mesures actuelles sont bien appliquées.

Ecart important de communication interne

Nous pouvons constater que dans cette école, des mesures et des consignes de sécurité sont données, mais qu'il y a un énorme écart de communication entre ce qui est mis en place par le service informatique, ce que les utilisateurs estiment qu'il devrait être fait et ce qu'ils perçoivent.

6.2.2 Haute Ecole de Gestion[38]

Cette Haute Ecole forme des professionnels de l'économie et des services. Dans cette école, nous avons des professionnels qui cherchent, créent et transforment l'information afin de créer une valeur ajoutée.

Communication succincte

Après avoir interviewé quatre personnes au sein du corps administratif et enseignant, nous avons pu constater qu'il n'y a aucune sensibilisation qui est faite lors de l'engagement d'un nouveau collaborateur au sein de l'école. Le directeur adjoint explique que le service informatique et la direction se base sur les us et coutumes des utilisateurs, qu'il n'y a donc pas besoin les en informer.

Le service informatique, néanmoins, explique envoyer de temps en temps des courriers électroniques de prévention ou de rappel pour avertir l'ensemble des collaborateurs. Ce que les utilisateurs confirment.

Le directeur adjoint ajoute tout de même qu'une charte informatique, disponible au même endroit que pour la HEDS, était soumise aux nouveaux employés à leur arrivée, mais celle-ci à dû être abandonnée pour des raisons légales. C'est pourquoi les mesures de sécurité ne sont plus communiquées à l'engagement.

Prises de mesures personnelles

Cependant, chaque collaborateur interrogé prend tout de même des mesures, en plus de celles communiquées lors des rappels, pour mieux sécuriser l'information.

En effet, même si certains utilisateurs ne sont pas forcément sensibiliser à des manipulations sécuritaires sur leur outil de travail, d'autres ont un bagage qui leur permettent d'appliquer des mesures de sécurité judicieuses de par leur expérience professionnelle parallèle ou antérieure. De plus, ceux qui font preuve de plus de conscience en matière de sécurité que d'autres, sont ceux qui lisent toutes les informations émises par leurs collaborateurs et qui sont attentifs à la vie de l'entreprise. Effectivement, un employé bien informé sur ses collègues et les dernières nouvelles de la compagnie peut mieux estimer le degré de risque en manipulant des mails ou des liens infectés. De plus, il sera attentif à d'éventuel intrus au sein d'un bureau ou sur des demandes faites par des personnes malveillantes.

Toutefois, bien que les responsables concernés n'estiment pas à tort que les utilisateurs aient déjà un bagage de par leur formation ou l'habitude d'un ordinateur,

[38] Vous trouverez les interviews des collaborateurs de la HEG à l'annexe 5

encore beaucoup ne sont pas forcément conscients des risques qu'ils prennent suivant l'utilisation qu'ils en font. Ils n'ont peut-être même pas été sensibilisés du tout, que ce soit à leur ancien poste ou durant leur apprentissage avec un ordinateur.

Certains, mêmes, demandent des explications à leur collègue afin de pouvoir appliquer certains gestes pour sécuriser l'information, ce qui contribuent à perpétuer d'éventuels mauvais usages.

Vision des utilisateurs face aux mesures de sécurité conseillées

Tous les collaborateurs interviewés comprennent très bien pour qu'elle raison ils doivent faire attention, chacun les applique dans la mesure de ses connaissances et par conscience professionnelle. Il n'y a donc pas de problème de ce côté-là. Cependant, ils estiment qu'ils manquent d'explications sur les mesures à prendre ou les manipulations à ne pas faire sur un ordinateur. Néanmoins, ils supposent que si des mesures plus approfondies n'ont pas été mises en place, c'est notamment par manque de ressources ou parce que les principaux concernés ont estimés qu'ils étaient déjà formés. Ce dernier point rejoint l'état d'esprit du directeur adjoint.

Vision du service informatique face aux mesures de sécurité appliquées

Selon le responsable, les utilisateurs ne sont pas encore assez attentif quand ils manipulent l'ordinateur. Il y aurait encore de la sensibilisation à faire au sein de l'école. En effet, le service informatique explique avoir mis en place des mesures techniques, afin de sécuriser un maximum l'information, mais peu de collaborateurs sont au courant de ces mesures et parfois, ils prennent des initiatives qui peuvent nuire à la sécurité.

Manque flagrant de communication et de formation interne

Nous constatons que dans cette école, il y a très peu de communication concernant la sécurité de l'information auprès des utilisateurs. Elle se fait seulement lorsque des incidents ou de nouvelles menaces apparaissent. C'est pourquoi les utilisateurs prennent des mesures personnelles selon leurs habitudes, mais ne sont pas forcément conscients de la prise de risque qu'ils font prend au SI de l'école.

Il y a donc un fossé entre ce que pense communiquer le service informatique et ce que les utilisateurs perçoivent.

6.2.3 Impacts de la sensibilisation en HES

Après l'interview des collaborateurs de ces deux écoles, nous avons perçu un manque assez important d'information, de communication et de formation de la part du service informatique et de la direction de l'école. Alors pourquoi y-a-t-il encore cet écart de vision entre les responsables de la sécurité et les utilisateurs ? Quels impacts cela a-t-il sur les utilisateurs et le SI ?

Charte informatique inutile actuellement

Nous pouvons relever plusieurs points sur la manière dont la communication est faite. En effet, premièrement une charte a été établie, mais aucun collaborateur ne l'a lu ces cinq dernières années. De plus, elle n'est plus expliquée lors de l'embauche d'un nouvel employé. Cet état de fait à un impact sur le collaborateur, il ne sait pas du tout à quoi s'en tenir en matière de sécurité. Il va donc mettre en place ce qu'il connait et tant pis pour les éventuelles erreurs ou manquement à la sécurité. La direction devrait au moins la soumettre aux nouveaux employés ou la leur expliquer lors de leur engagement, afin de partager sa vision de la sécurité avec ses collaborateurs.

Courriers électroniques perdus dans la masse

Deuxièmement, le service informatique envoie que des courriers électroniques de rappels ou d'avertissement. C'est une bonne manière de communiquer, cependant, ce n'est qu'une transmission de message, il n'y pas de suivi. Généralement, ce genre de message se perd dans la masse des messages non lus, parce que les collaborateurs n'ont pas forcément le temps de les lire. Un courrier électronique transmis à l'ensemble des collaborateurs est devenu banal, donc l'impact est minime sur l'utilisateur. Il faudrait créer avant cela une communication qui puissent les rendre attentif au fait que c'est important de lire un message provenant du service informatique.

Explications et formations inexistantes

Troisièmement, il n'y a aucune explication sur les enjeux de la sécurité des informations au sein de l'école. Tout le monde est évidemment conscient qu'il est nécessaire de sécuriser les informations, mais ils n'ont pas reçu de communication exacte à ce sujet. Il y a un manque concernant la communication de base, afin de pouvoir amener tout le monde au même niveau. Ainsi, la direction pourra créer une synergie et une culture d'entreprise en matière de protection des informations. Donc, chacun se sentira concerner dans le processus de sécurité.

Ensuite, il n'y a pas de formation explicite, le service informatique explique seulement aux collaborateurs qui le demandent, comment faire certaines manipulations de sécurité avec leur ordinateur. Une équipe devrait donc être créée afin d'établir un

programme de formation, qui permet d'intégrer les usages sécuritaires et d'impliquer les utilisateurs, afin qu'ils sachent comment faire, comment réagir, et comment réduire l'impact de leurs manipulations.

Message de sécurité flou

Quatrièmement, le fait qu'il manque d'information et d'explications, contribuent à laisser les utilisateurs dans le flou concernant la vision de la sécurité de la direction et du service informatique de l'école. Il n'y a pas de structure, ni message clair qui est transmis aux utilisateurs, ce qui les confortent dans les habitudes prises avec leur outil de travail. Il faudrait que la direction établisse un document de type politique de sécurité, afin de diffuser sa vision de la sécurité au travers de l'infrastructure, et ainsi cela créera une base pour la suite de la sensibilisation et un message clair auprès des utilisateurs.

Pas de responsable ne charge de la SSI

Enfin, il n'y a pas de responsable clairement défini en charge de la sécurité du système d'information. C'est le service informatique qui dans les deux cas a pour tâche d'informer les collaborateurs en matière de sécurité. Il transmet des informations seulement quand cela est réellement nécessaire, mais pas de manière continue comme cela est préconisé, afin de créer une sensibilisation auprès des utilisateurs.

6.2.4 Conclusion

En définitive, nous remarquons qu'il n'y a pas de culture de protection des informations au sein des deux HES, aucune des deux directions ne transmettent clairement leurs visions de la sécurité à leurs collaborateurs. Les moyens de communication et de formation sont inadaptés, voir inexistants, les utilisateurs ne reçoivent pas de messages précis concernant la sécurité de leurs informations professionnelles et ne connaissent pas forcément les bonnes pratiques à mettre en œuvre pour éviter de faire prendre des risques à l'école.

Ce manque de sensibilisation auprès des utilisateurs en matière de sécurité du système d'information, crée un écart important entre ce que pense communiquer le service informatique et les collaborateurs. Cela amène donc les utilisateurs et la direction a supposé qu'il faille agir selon ce que le bon sens et la conscience professionnelle voudrait.

7. Mise en place dans un cas concret

L'objectif de ce chapitre est de proposer une manière de réduire l'écart de communication qu'il y a entre le centre informatique et les utilisateurs du SI d'une HES concernant la politique de sécurité implantée en utilisant la sensibilisation. Les collaborateurs doivent pouvoir bénéficier d'un meilleur programme de sensibilisation, pour remettre à niveau leurs connaissances en matière de sécurité, dans le but de réduire les risques énumérés tout au long de ce travail.

Nous proposons des améliorations qui motiveraient tous les collaborateurs à user des bonnes pratiques de sécurité recommandées par le service informatique. Cette campagne doit leur faire prendre conscience qu'ils font partie intégrante du processus de SSI installé par l'entreprise.

Nous suggérons de structurer le programme de sensibilisation de la manière suivante :

- Phase 1 : Planification ;
- Phase 2 : Conception ;
- Phase 3 : Diffusion ;
- Phase 4 : Evaluation ;
- Phase 5 : Maintenance.

De plus nous proposons, de partager la diffusion en deux étapes :

- Etape 1 : piloter le programme avec un groupe limité à une dizaine d'utilisateurs cibles, pour s'assurer de la pertinence du contenu et son déroulement. Suite à ce pilote, nous procéderons aux améliorations nécessaires.
- Etape 2 : mettre en œuvre pour toute l'école et ce de manière incrémentale par groupe.

La diffusion du programme pour chacune des deux étapes se fera suivant les quatre axes suivants :

- Axe 1 : Information
- Axe 2 : Communication
- Axe 3 : Formation
- Axe 4 : Evaluation

Les points suivants décrivent chacune des phases et leur contenu.

7.1 Planification de la sensibilisation

Tout d'abord, il faut constituer une équipe pour mener à bien une campagne de sensibilisation. Pour cela, nous suggérons de puiser dans les ressources de l'école.

7.1.1 Acteurs impliqués

Nous proposons de constituer une équipe qui sera composée de ressources provenant des différents services ci-après.

Tableau 4 : Acteurs impliqués et leurs responsabilités

Métiers	Pourquoi	Responsabilités
Chef de projet	Pour coordonner tout le programme.	De créer le programme et de coordonner toutes les activités et ressources pour assurer le succès du lancement de ce programme.
Service informatique	Il est en charge de la gestion du système informatique de l'école et de sa sécurité.	Etablir une politique de sécurité. Etablir les points de sécurité à communiquer.
Service communication	Ses compétences sont utiles, car il est en charge de la gestion des communications au travers de l'école. De plus, il travaille en étroite collaboration avec un graphiste et un webmaster.	Etablir la communication (messages) concernant le projet à faire passer auprès des collaborateurs. Etablir le choix des supports d'information, de communication, de formation en rapport avec les points de sécurité établis aux préalables.
Graphiste	Il s'occupe du graphisme des différentes campagnes de communication à travers la HEDS, ses compétences sont donc utile pour ce projet.	Etablir les graphismes utiles à la communication sur plusieurs supports en rapport avec les points de sécurité établis aux préalables.
Webmaster	Il s'occupe de la gestion de l'intranet des deux HES.	Etablir les supports virtuels pour la communication en rapport avec les points à sécuriser établis aux préalables.
Ressources humaines	Il s'occupe de la gestion des employés, ses services seront appréciés lors de l'engagement des nouveaux employés et par la suite.	Sa responsabilité sera : Mettre en œuvre la communication lors des embauches, des réunions de présentation de l'entreprise.

7.1.2 Organisation

Ensuite, nous avons établi un planning, qui permet de visualiser dans le temps les différentes tâches à accomplir pour la campagne de sensibilisation. Il faut, cependant, prendre en compte qu'il reflète une situation « idéale ». C'est-à-dire qu'il faut supposer que la direction ait donné son accord, et que les collaborateurs dont nous avons besoin, sont libres aux moments voulus et peuvent consacrer une partie de leur temps de travail à la réalisation de ce projet.

Toutefois, ce plan n'est pas optimisé, certaines tâches peuvent être faites en parallèle par des acteurs différents. De plus, le nombre de jours proposé est approximatif, car nous n'avons pas les moyens pour déterminé exactement le temps pour effectuer une tâche.

Voici dans les grandes lignes le planning proposé :

- Phase 1[39] : Planification – Durée 3 semaines ;
- Phase 2[40] : Conception – Durée 11 semaines ;
- Phase 3 : Diffusion
    - Etape 1[41] (pilote) : Durée 12 semaines ;
    - Etape 2[42] (réelle) : Durée 24 semaines (dû au nombre d'utilisateurs) ;
- Phase 4 : Evaluation – Durée
    - Etape 1[43] (pilote) : 5 semaines (inclus améliorations) ;
    - Etape 2[44](réelle) : 5 semaines (inclus améliorations) ;
- Phase 5[45] : Maintenance. – Durée continue.

7.1.3 Evaluation du budget à obtenir

Le budget pour cette campagne est constitué entièrement de ressources disponibles au sein de l'école. Pour les ressources matérielles dont le coût est minimal, il devrait est absorbé dans les budgets déjà existants.

En ce qui concerne les ressources humaines, nous avons toutefois, voulu représenter financièrement le temps passé par l'équipe de projet afin de nous faire une idée sur le coût, bien que selon les entreprises, les ressources internes ne sont pas toujours

[39] Vous trouverez la planification de la phase 1, ainsi que son budget à l'annexe 6

[40] Vous trouverez la planification de la phase 2, ainsi que son budget à l'annexe 7

[41] Vous trouverez la planification de la phase 3 – étape 1, ainsi que son budget à l'annexe 8

[42] Vous trouverez la planification de la phase 3 – étape 2, ainsi que son budget à l'annexe 9

[43] Vous trouverez la planification de la phase 4 – étape 1, ainsi que son budget à l'annexe 10

[44] Vous trouverez la planification de la phase 4 – étape 2, ainsi que son budget à l'annexe 11

[45] Vous trouverez la planification de la phase 5, ainsi que son budget à l'annexe 12

facturées au projet. Nous avons déterminé que le coût moyen d'un collaborateur pour ce projet est d'environ 100'000 francs par année et travaille 210 jours par an, ce qui revient à environ 476 CHF par jour. Nous avons estimé la charge de travail effective jusqu'à la fin de la phase 4 est d'environ 152 jours (effort), ce qui donne un coût approximatif de 72'000 CHF en ressources humaines.

7.2 Conception du programme de sensibilisation

Ensuite, nous développons le programme de sensibilisation. Nous devons comme il est préconisé par l'ENISA, et Microsoft, ciblé les utilisateurs afin de leur proposer un contenu qui les touchent directement par des canaux de communication adaptés et ainsi les intéresser à la sécurité des informations qu'ils manipulent.

7.2.1 Groupes d'utilisateurs cibles

Premièrement, afin de choisir la bonne forme de communication dont ils ont besoin, il faut définir les groupes ciblés d'utilisateurs que nous souhaitons atteindre. Au sein de l'école, la communication en matière de sécurité touche trop globalement les utilisateurs, sans prendre en compte leur besoin relatifs à leurs tâches.

En effet, chaque type d'utilisateur n'a pas les mêmes besoins en matière de sensibilisation. Un membre de la direction n'utilise pas les mêmes informations qu'un professeur. C'est pourquoi, en prenant en compte la structure des employés au sein d'une école telle qu'une HES, nous proposons de faire quatre groupes cibles ayant des besoins de sensibilisation et de formation différents.

Tableau 5 : Groupes d'utilisateurs ciblés et les objectifs de sensibilisation

Groupes cibles	Niveaux de sensibilisation	Objectifs de la sensibilisation
Direction	Ils ont un niveau de conscience élevé du à leurs responsabilités.	Accroitre la compréhension d'un tel projet. S'assurer de leur engagement et support lors de la campagne. Rester informés sur les dangers des technologies utilisées au sein de l'établissement, pour permettre des prises de décisions stratégiques. Rester eux-mêmes informés et formés.
Personnel administratif et technique	Certains ne se rendent pas encore bien compte des conséquences de leurs manipulations sur les outils informatiques.	Rendre attentif aux risques et aux dangers auquel est exposé le SI de l'école par leur propre utilisation. Mettre en place une manipulation plus sécurisée du système.
Professeurs et assistants	Certains ne se rendent pas encore bien compte des conséquences de leurs manipulations sur les outils informatiques.	Rendre attentif aux risques et aux dangers auquel est exposé le SI de l'école par leur propre utilisation. Mettre en place une manipulation plus sécurisée du système.
Professeurs, assistants et personnel informatiques	Ils ont un niveau de conscience plus élevée due à leur métier.	Rendre attentif aux failles de sécurité qu'il y a encore de par leur manipulation du système.

7.2.2 Messages ciblés

Ensuite, ces groupes doivent comprendre qu'ils ont la sécurité des informations de l'école entre leurs mains, que les informations qu'ils manipulent doivent rester confidentielles, disponibles et intègres pour leur travail et la réputation de l'école. C'est pourquoi, la communication lors du programme doit utiliser un message qui les touche.

Tableau 6 : Messages à faire passer auprès des groupes cibles

Groupe cible	Messages
Direction	*« Intégrez vos collaborateurs à la sécurité des informations de votre école. »* *« Prenez des décisions sur les technologies de l'information de votre école en toute connaissance de cause. »* *« Restez un élément important de la sécurité des informations de votre école. »*
Personnel administratif et technique	*« Devenez un élément important de la sécurité des informations de votre école. »*
Professeurs et assistants	*« Devenez un élément important de la sécurité des informations de votre école. »*
Personnel Informatique (incluant professeurs et assistants)	*« Restez un élément important de la sécurité des informations de votre école. »*

7.2.3 Contenu adapté de la sensibilisation

Deuxièmement, il faut définir le contenu de la sensibilisation à laquelle ces groupes seront soumis. Actuellement, au sein de l'école, le contenu est le même pour chacun et reste très minime. En effet, ces groupes ont des utilisations et des connaissances des technologies de l'information différentes. Un professeur informaticien aura plus de connaissances sur ces technologies qu'un professeur de français. C'est pourquoi en prenant en compte les tâches des collaborateurs de l'école, nous pourrions ciblés le contenu de la sensibilisation selon le tableau ci-dessous.

A noter que la sensibilisation aux virus, à l'hameçonnage et aux logiciels malveillants, ce ferait de toute façon à l'intérieur de ces thèmes et par le biais des informations et communications envoyer par le centre informatique lorsqu'il le juge opportun.

Voici une suggestion de thèmes qui pourraient être traités lors durant la première année du programme.

Tableau 7 : Contenu de la sensibilisation adapté aux groupes cibles

Groupes cibles	Contenu de la sensibilisation
Direction	• Sécuriser le poste de travail : – médias mobiles • Sécurité en dehors du bureau • Téléphones mobiles • Documents papiers
Personnel administratif et technique	• Sécuriser le poste de travail : – mot de passe – médias mobiles • Utiliser les outils à des fins professionnelles • Ingénierie sociale • Documents papiers
Professeurs et assistants	• Sécuriser le poste de travail : – mot de passe – médias mobiles • Utiliser les outils à des fins professionnelles • Sécurité en dehors du bureau • Ingénierie sociale • Documents papiers
Personnel Informatique (incluant professeurs et assistants)	• Utiliser les outils à des fins professionnelles • Ingénierie sociale • Sécurité en dehors du bureau • Documents papiers

En effet, pour les membres de la direction, ils sont souvent amenés à utiliser leurs téléphones mobiles pour leur travail, ils sont amenés par leur responsabilité à se déplacer à l'extérieur de l'école ou à travailler à la maison et ont parfois besoin d'utiliser différents supports pour la sauvegarde de leur travail ou l'échange d'informations avec leurs partenaires de travail. Ils traitent aussi des documents confidentiels.

Ensuite, nous en venons au cœur des collaborateurs qui ont besoin d'être sensibilisés pour un nombre de points plus importants que leurs autres collègues. Ces deux groupes, les professeurs et le personnel administratif et technique, sont des groupes très hétérogènes avec des responsabilités et des tâches qui diffèrent et des

connaissances toutes aussi variées. C'est pourquoi nous ne pouvons pas plus les subdiviser.

Effectivement, un grand nombre de ces utilisateurs ont encore des difficultés avec la sécurité de leurs outils informatiques. Beaucoup utilisent leurs outils informatiques à des fins personnelles pendant leurs pauses, connectent des médias sur leur poste ou lancent des impressions et oublient d'aller récupérer les documents. Ensuite, il y a aussi le problème d'ingénierie sociale qui est posé, car beaucoup pour être serviable répondent à des questions sensibles par téléphone ou par courrier électronique sans se demander si l'interlocuteur est bien celui qu'il prêtant être, pour ne citer qu'un exemple parmi l'immense palette de possibilités de l'ingénieur sociale.

En revanche, en ce qui concerne la sécurité en dehors du bureau, nous avons estimé que les professeurs sont amenés à se déplacer plus souvent ou à utiliser chez eux des applications pour leur travail que le personnel administratif et technique ne fait pas. Généralement, ceux-ci ne travaillent pas chez eux ou quand ils se déplacent c'est souvent dans un endroit similaire à l'environnement de l'école.

Pour finir avec les informaticiens, ayant déjà beaucoup de connaissances sur les faiblesses des technologies de l'information, il est préférable d'axer la sensibilisation sur des points où ils ont aussi de petites faiblesses en tant qu'être humain. Comme le fait que par exemple, l'ingénierie sociale prend différentes formes, lorsqu'ils utilisent des outils de l'école en dehors, il faut qu'ils fassent attention et les documents imprimés doivent être récupérés immédiatement et détruits si ceux-ci présentent une sensibilité.

7.2.4 Moyens de communication adaptés

Troisièmement, il faudrait définir des moyens de communication adaptés à la structure de l'école, aux groupes ciblés et au contenu de la sensibilisation. Au sein de l'école, les seuls canaux de communication qu'ils utilisent sont le courrier électronique ou oralement lorsque l'utilisateur reçoit des informations de son centre informatique.

En effet, le moyen de communiquer est primordial afin que les individus auxquels nous nous adressons intègrent le message que nous souhaitons faire passer. Il faut que les collaborateurs puissent prendre le temps de s'informer, d'apprendre et de se former pour retenir et appliquer l'essentiel du programme de sensibilisation mis en œuvre.

C'est pourquoi nous avons sélectionné les différents canaux de communication adaptés aux types d'utilisateurs, à l'infrastructure d'une HES, et trois des quatre

dimensions qu'un programme de sensibilisation doit avoir. A l'annexe 13, vous trouverez le tableau avec les canaux non retenus et leurs justifications.

Tableau 8 : Canaux de sensibilisation adaptés aux utilisateurs

Canaux	**Pourquoi**
Information	
Direction	Soutenir et entretenir le message de sécurité de manière orale ou écrite.
Chef de groupe	Entretenir le message de sécurité de manière orale ou écrite.
Règlement	Les règlements existent déjà.
Charte informatique	La charte informatique existe déjà.
Contrat	Les contrats existent déjà.
Politique de sécurité	Elle prend du temps, des ressources, mais elle est essentielle à la diffusion de la sécurité. Donc elle est importante à mettre en place.
Conférence	Il faut prendre du temps pour établir le contenu, trouver les collaborateurs responsables, agender un moment qui convienne à une majorité de collaborateurs concernés. Mais cela fait parti du processus de sensibilisation, afin que les employés se sentent impliqués dans le programme.
Communication	
Questionnaire	Il faut prendre le temps pour établir des questionnaires axés sur les différents sujets de sécurité, mais le support ne coût rien, surtout si celui-ci se trouve en ligne.
Site intranet	L'intranet existe déjà, il faut juste prendre le temps de stocker et mettre en forme le contenu de la sensibilisation.
Ecran de veille	Les écrans de veille en eux-mêmes ne coûtent rien et ils sont installés par le service informatique.
Fond d'écran	Idem que pour les écrans de veille.
Message sur l'ordinateur	Les messages ne coûtent rien, il faut juste prendre le temps de personnaliser un message destiné à un collaborateur précis.
Courrier électronique	Les courriers électroniques ne coûtent rien et sont envoyés par le service informatique, dans le cadre de leur mission.
Newsletter	Les newsletters ne coûtent rien et sont envoyés par le service de communication, dans le cadre de leur mission.
Affiches	Les affiches prennent du temps pour leur conception et le support et l'impression peuvent coûter. Mais ensuite, leur contenu peut être repris sur d'autres supports.

Helpdesk	C'est un moyen de communication qui existe déjà et il est amené avec les interventions que le service a à fournir.
Formation	
Mise en situation	Il faut en établir le contenu, les collaborateurs qui les dispensent, occuper une salle, agender la mise en situation, et suivant ce que le programme contient, compter les coûts en support matériel.
Atelier	Idem que pour les mises en situation.

Vous trouverez en annexe 14, un exemple[46] de moyen de communication qui pourrait être utilisés au sein des deux HES.

7.3 Diffusion du programme de sensibilisation

Cette phase du programme est la mise en œuvre visible de la sensibilisation. Nous allons donc présenter aux utilisateurs le programme de sensibilisation.

La diffusion se fera en deux étapes :

- Etape 1 : piloter le programme avec un groupe limité à une dizaine d'utilisateurs cibles, pour s'assurer de la pertinence du contenu et son déroulement. Suite à ce pilote, nous procéderons aux améliorations nécessaires.
- Etape 2 : mettre en œuvre pour toute l'école et ce de manière incrémentale, par groupe.

7.4 Evaluation du programme de sensibilisation

L'évaluation se fera autant après l'étape de pilotage que la mise en œuvre.

Il y a deux sortes d'évaluation possibles :

Pour la première, il s'agit de faire évaluer à chaque collaborateur comment il a perçu cette sensibilisation. Les questions qui pourraient être posées par l'intermédiaire d'un questionnaire anonyme, sont les suivantes :

- Avez-vous compris l'importance de cette sensibilisation ?
- Les objectifs de cette campagne vous ont-ils été clairement expliqués ?
- Avez-vous été touchés par le système de communications mis en place ?
- Avez-vous été touchés par le contenu de la sensibilisation proposée ?
- Les points abordés vous ont-ils intéressés ?

[46] Exemple de communication au moyen d'affiches tiré du site de CASES, qui proposent une réflexion sur son comportement face à la sécurité de son poste de travail :

CYBERWORLD AWARENESS & SECURITY SURVEY ENHANCEMENT SERVICES. Se protéger [en ligne]. https://www.cases.lu/fr/la-sensibilisation-et-la-formation.html (consulté le 02.07.2013)

- Avez-vous appris des bonnes pratiques jusque là inconnues ?
- Avez-vous des suggestions ?
- Avez-vous des points négatifs dont vous souhaitez faire part ?
- Comprenez-vous mieux l'importance de la sécurité ?
- Allez-vous mettre en pratique la sensibilisation reçue ?

Pour la seconde, il s'agit d'évaluer si la campagne de sensibilisation à porter ses fruits, en utilisant les moyens suivants :

Tableau 9 : Moyens d'évaluation de la campagne de sensibilisation

Moyens	**Explications**
Questionnaire	Etablir un questionnaire avec des questions comme : *« Que feriez-vous si… »* à choix multiple. Les faire remplir à chaque collaborateur.
Rapport d'incidents	Grâce aux rapports d'incidents, l'équipe en charge de la sécurité peut établir s'il y a plus ou moins de fautes commises par leurs collaborateurs. L'audit est à faire sur le long terme.
Helpdesk	Ce sont les collaborateurs qui peuvent donner un ressenti global sur la prise de conscience de leurs collègues concernant leur sensibilisation. Ils sont proches d'eux et donc en direct avec le terrain.

Ces moyens ne sont pas exhaustifs, et correspondent à l'infrastructure d'une HES.

7.4.1 Besoin de sensibilisation

Les questionnaires pourraient aussi permettre d'évaluer le niveau de chaque collaborateur et leur permettre de ne pas avoir besoin de participer une ou deux fois au programme de sensibilisation. Ils seraient ainsi dispensés de participer au programme de sensibilisation tant qu'ils seront jugés « avertis ».

7.5 Maintenance sur le long terme

Pour finir, cette dernière phase, consiste à maintenir le programme de sensibilisation sur le long terme afin de constituer une culture solide de la sécurité des informations au sein de l'école.

7.5.1 Fréquence du programme et des révisions

En effet, une campagne de sensibilisation n'est pas un programme à faire une fois de temps en temps, c'est un programme à dispenser et à mettre à jour continuellement. Comme l'a proposé lors de notre interview le directeur adjoint de la HEG, ce programme pourrait être intégré au processus Qualité de l'école et donc être revue tous les dix-huit mois comme tous processus Qualité. De plus, il faudrait nommer un collaborateur qui en serait chargé. Un employé ayant déjà collaboré au programme, comme aux ressources humaines ou au service de communication. Ainsi, les écoles auront, elles aussi, un « responsable de la sécurité des systèmes d'information », comme cela ce fait ailleurs. Ce responsable devrait être nommé au plus pour la maintenance du programme.

7.5.2 Contenu de la communication de sensibilisation

La communication devrait être proposée sur l'intranet de l'école afin que les collaborateurs puissent s'informer en tout temps. En effet, si nous nous basons sur ce que déplorent certains interviewés, c'est le manque de récapitulatif pour se remémorer les points de sécurité qu'ils auraient oubliés.

De plus, la communication de rappels ou d'avertissement concernant de nouvelles menaces ou nouveautés technologiques devrait se faire de manière continue au sein de l'école, afin de coller au plus prés de l'actualité. Le service informatique ou le service de communication interne devrait en avoir la responsabilité.

7.5.3 Nouveaux collaborateurs

Pour les nouveaux employés, les ressources humaines devraient les informer de la vision de l'école en matière de sécurité de l'information lors de la signature de leur contrat. Elles leur demanderont de lire la charte informatique, qui indiquera où trouver le site intranet contenant les supports de sensibilisation. Ensuite, elles devraient résumer lors de la présentation de l'école aux nouveaux collaborateurs la vision de l'école en matière de sécurité. Enfin, les nouveaux arrivés intègreraient le processus mis en place pour les autres employés.

7.6 Conclusion

Avec ces différentes propositions, les utilisateurs deviendront des collaborateurs avertis et l'écart de vision de la SSI pourra être réduit entre les utilisateurs, le service informatique et la direction.

Toutefois, comme nous l'avons constaté, cela demande du temps pour les ressources internes, ainsi qu'une volonté de la direction pour mettre en œuvre ce programme de sensibilisation. En plus, comme nous l'avons vu les sujets de sensibilisation sont nombreux et ne pourront donc pas tous être pris en compte en même temps. C'est pourquoi, l'école devrait identifier les priorités ainsi que des *« quick-wins »*[47] à mettre en place, pour obtenir des résultats plus rapidement, et régler les problèmes les plus importants. Il faudrait par exemple commencer tout simplement par informer les collaborateurs sur la sécurité de leur poste de travail et des documents qui restent sur les copieurs, nous pensons que ce serait déjà un premier pas.

[47] Ce sont des mesures à effet rapide.

8. Synthèse

En conclusion, ce qu'il faut retenir pour réduire l'impact du jugement de l'être humain et de ses actes sur le système d'information de l'entreprise, c'est de partager la vision de l'entreprise en matière de sécurité du système d'information, dès l'engagement d'un collaborateur. Qu'afin de mener à bien une campagne de sensibilisation en un programme structuré et reconnu, il s'agit d'obtenir le soutien des instances dirigeantes pour légitimer ce programme de sensibilisation au travers de l'entreprise.

Ensuite, à travers ce programme, établir, un processus pour informer et communiquer sur l'importance de l'information et son rôle névralgique dans les activités de l'entreprise, des risques qu'elle encourt et des conséquences des actes humains. Puis, de former les collaborateurs afin de leur inculquer une véritable compréhension des bonnes pratiques de sécurité, par des moyens de communication adaptés.

Pour finir, maintenir le processus de sensibilisation et d'évaluation en continue au sein de l'entreprise, afin d'établir et impliquer les collaborateurs dans la culture de la sécurité du système d'information de l'entité. Et par conséquent, en faire des utilisateurs avertis, et donc un atout pour la sécurité de l'entreprise.

Bibliographie

Articles en ligne :

- GRATIOLET, François. Sensibilisation à la cyber-sécurité : se prémunir des vulnérabilités d'origine humaine. In : *Le Cercle – Les Echos* [en ligne]. 2013. http://lecercle.lesechos.fr/entrepreneur/tendances-innovation/221177184/sensibilisation-a-cyber-securite-premunir-vulnerabilites (consulté le 24.08.2013)

- KARSENTI, Thierry, HASSID, Olivier, RONDEL, Philippe. Sécurité informatique- La prévention des menaces en entreprise. In : *L'info – Expoprotection* [en ligne]. 2012. http://www.info.expoprotection.com/?IdNode=1308&Zoom=ad64f6f5c65af1a49d444f2b8346dd33 (consulté le 10.07.2013)

Cours :

- AÏDONIDIS-FLÜCKIGER, Christine. *Urbanisation des SI* [présentation PowerPoint]. 2013. Supports de cours : 626-1 : Urbanisation des SI, Haute Ecole de Gestion de Genève, filière Informatique de gestion, année académique 2012-2013.

- HAURI, Rolf. *Gouvernance de la sécurité* [présentation PowerPoint]. 2011. Supports de cours : 634-2 Gouvernance de la sécurité, Haute Ecole de Gestion de Genève, filière Informatique de gestion, année académique 2010-2011.

Livres :

- BOULET, Patrick. *Management de la sécurité du SI*. Paris : Hermès Sciences, 2007. 246 p. : ill. (Management et Informatique)

- CALE, Stéphane, TOUITOU, Philippe. *La sécurité informatique : réponses techniques, organisationnelles et juridiques*. Paris : Hermès Sciences, 2007. 282 p. : ill. (Management et Informatique)

- HARLE, Thierry, SKRABACZ, Florent. *Clés pour la sécurité des SI*. Paris : Hermès Sciences, 2004. 296 p. : ill. (Management et Informatique)

- PILLOU, Jean-François, BAY, Jean-Philippe. *Tout sur la Sécurité informatique*. 2ème éd. Paris : DUNOD, 2005 -2009. 232 p. (Commentçamarche.net)

Livres électroniques :

- BENNASAR, Matthieu, BRIGAUD, Julien, COMBES, Létitia. *Sensibilisation à la sécurité de l'information 2.0* [en ligne]. Livre Blanc. PARIS : LEXSI – INNOVATIVE SECURTIY, 2013. 18 p. https://www.lexsi.fr/sites/default/files/publications/lb_sensibilisation_a_la_securite_de_linformation_2.0.pdf (consulté le 04.06.2013)

- DOUCENDE, Bruno. *Sécurité des Systèmes d'Information* [en ligne]. Livre Blanc. Marseille : Groupe 4, 4IM SAS, 2008. 32 p. http://www.globalsecuritymag.fr/IMG/pdf/Livre_Blanc_SSI_v1.pdf (consulté le 30.07.2013)

Norme :

- ORGANISATION INTERNATIONALE DE LA NORMALISATION (ISO). *Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour la gestion de la sécurité de l'information*. 1ère éd. Suisse : ISO, 2005. 134 p. Norme Internationale ISO/CEI 27002:2005 (F).

Sites web :

- CERN. Posters de sensibilisation à la sécurité informatique [en ligne]. https://security.web.cern.ch/security/training/fr/posters.shtml (consulté le 02.07.2013)

- CLUSIF. Le rôle de l'organisation humaine dans la SSI. In : Les synthèses du CLUSIF [en ligne]. Publié le 20 juin 2013. https://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-Humain-SSI-2013-Synthese.pdf (consulté le 29.07.2013)

- COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES. Guide – La sécurité des données personnelles [en ligne]. Edition 2010. Inconnu : CNIL, 2010. 48 p. http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Guide_securite-VD.pdf (consulté le 05.07.2013)

- CONSIO-TECHNOLOGIES. Sensiwave, un nouveau lien entre l'entreprise et ces collaborateurs [en ligne]. http://www.conscio-technologies.com/?option=com_content&view=article&id=109&Itemid=92 (consulté le 16.09.2013)

- CYBERWORLD AWARENESS & SECURITY SURVEY ENHANCEMENT SERVICES. Se protéger [en ligne]. https://www.cases.lu/fr/la-sensibilisation-et-la-formation.html (consulté le 02.07.2013)

- DELOITTE, 2013. Blurring the lines – 2013 TMT Global Security Study [PDF]. 2013. In : Deloitte. http://www.deloitte.com/view/en_GX/global/industries/technology-media-telecommunications/a4f47802b967b310VgnVCM3000003456f70aRCRD.htm# (consulté le 29.07.2013)

- DUVAUCHELLE, Antoine pour l'Agence nationale de la sécurité des systèmes d'information. Guide d'hygiène informatique [en ligne]. 1ère éd. Paris : ANSSI, 2013. 52 p. http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf (consulté le 05.07.2013)

- ENISA. Le nouveau guide utilisateur : comment améliorer la sensibilisation à la sécurité de l'information. 2008, 110p. http://www.enisa.europa.eu/publications/archive/new-users-guide-fr (consulté le 05.07.2013)

- ERNST AND YOUNG, 2012. Fighting to close the gap – 2012 Global Information Security Survey [PDF]. 2012. In : PricewaterhouseCoopers. http://www.ey.com/Publication/vwLUAssets/Fighting_to_close_the_gap:_2012_Global_Information_Security_Survey/$FILE/2012_Global_Information_Security_Survey___Fighting_to_close_the_gap.pdf (consulté le 29.07.2013)

- EPFL. Campagne de sensibilisation à la Sécurité Informatique [en ligne]. https://secure-it.epfl.ch/sensi/ (consulté le 02.07.2013)

- GOMAS, Olivier, RAISIN, Yves, ROZIER, Richard. Le facteur humain. In : *CLUSIR Rhône-Alpes* [en ligne]. http://www.clusir-rha.fr/sites/default/files/upload/Lyon/SSI/CLUSIR_FACTEUR%20HUMAIN_161903.pdf (consulté le 29.07.2013)

- HAPSIS. La protection de vos informations dans un environnement complexe [en ligne]. http://www.se-force.com/index.php?option=com_content&view=article&id=116&Itemid=152 (consulté le 24.08.2013)

- HAUTE ECOLE SPECIALISEE DE SUISSE OCCIDENTALE. Qui sommes-nous [en ligne]. http://www.hes-so.ch/fr/sommes-nous-26.html (consulté le 02.07.2013)

- ILLAND, Joseph pour le Centre national de la recherche scientifique. Politique de Sécurité des Systèmes d'Information [en ligne]. 1ère éd. Inconnu : CNRS, 2006. 26 p. http://www.dgdr.cnrs.fr/fsd/securite-systemes/documentations_pdf/securite_systemes/pssi-v1.pdf (consulté le 05.07.2013)

- LARBI, Abdelkader. *Contribution à la mise en place d'un dispositif de veille stratégique dans une entreprise commerciale, Cas de NAFTAL* [en ligne]. 2006. Post Graduation Spécialisée en Management de l'information. Centre de Recherche sur l'Information Scientifique et Technique, Alger. http://www.memoireonline.com/04/08/1066/m_contribution-mise-en-place-dispositif-veille-strategique-naftal1.html (consulté le 29.07.2013)

- MELANI, 2012. Sûreté de l'information - Situation en Suisse et sur le plan international, Rapport semestriel 2012/I (janvier à juin) [PDF] In : Confédération suisse. http://www.melani.admin.ch/dokumentation/00123/00124/01526/index.html?lang=fr (consulté le 02.07.2013)

- MICROSOFT. Facteurs clés pour le développement de programmes efficaces de sensibilisation et de formation à la sécurité des informations. In : Sensibilisation à la sécurité [en ligne]. 2006. http://technet.microsoft.com/fr-fr/security/cc165442.aspx (consulté le 05.07.2013)

- ORGANISATION INTERNATIONALE DE NORMALISATION. Normes [en ligne]. http://www.iso.org/iso/fr/home/standards.htm (consulté le 05.07.2013)

- ORGANISATION INTERNATIONALE DE NORMALISATION. A propos de l'ISO [en ligne]. http://www.iso.org/iso/fr/home/standards.htm (consulté le 05.07.2013)

- PRICEWATERHOUSECOOPERS, 2008. Safeguarding the new currency of business – 2008 Global State of Information Security [PDF]. 2008. In : PricewaterhouseCoopers. http://www.pwc.fr//assets/files/pdf/2008/12/pwc_safeguarding_the_new_currency.pdf (consulté le 29.07.2013)

- PRICEWATERHOUSECOOPERS, 2011. Respect - but still restrained – 2011 Global State of Information Security Survey [PDF]. 2011. In : *PricewaterhouseCoopers.* http://www.pwc.fr//assets/files/pdf/2010/12/pwc_2011_it_security_survey_report.pdf (consulté le 29.07.2013)

- PRICEWATERHOUSECOOPERS, 2013. Tendance et enjeux de la sécurité de l'information – 2013 Global State of Information Security Survey [PDF]. 2013. In : *PricewaterhouseCoopers*. http://www.pwc.fr//assets/files/pdf/2013/03/pwc_global_state_information_security_survey.pdf (consulté le 29.07.2013)

- PRICEWATERHOUSECOOPERS, 2013. Changing the game, Key findings from 2013 Global State of Information Security Survey [PDF]. 2013. In : *PricewaterhouseCoopers*. http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/2013-giss-report.pdf (consulté le 29.07.2013)

- TERRANOVA. Sensibilisation Sécurité de l'Information [en ligne]. http://www.tnawareness.com/fr/securite-information (consulté le 16.09.2013)

- TONINATO, Aurélie. La Haute Ecole de gestion victime d'une grosse fraude : 270 élèves doivent repasser l'examen ! In : *Tribune de Genève* [en ligne]. Dernière modification le 21.02.2012. http://www.tdg.ch/geneve/actu-genevoise/haute-ecole-gestion-victime-grosse-fraude-270-eleves-doivent-repasser-lexamen/story/28574846 (consulté le 30.07.2013)

- WIKIPEDIA. Facteur de risque. In : *Wikipédia* [en ligne]. Dernière modification de cette page le 13 mars 2013 à 09 :27. http://fr.wikipedia.org/wiki/Facteur_de_risque (consulté le 24.08.2013)

- WIKITIONNAIRE. Sensibilisation. In : *Wikitionnaire* [en ligne]. Dernière modification de cette page le 16 août 2012 à 19 :02. http://fr.wiktionary.org/wiki/sensibilisation (consulté le 21.06.2013)

Travail de Bachelor :

MARQUES, Henrique. *Se prémunir contre les menaces provenant de ses propres employés*. 2008. 70 p. Mémoire, Informatique de Gestion, Haute Ecole de Gestion de Genève. 2008.

Vidéo en ligne :

Deloitte. Situation de cyber attaque susceptible de menacer votre entreprise [en ligne]. http://www.deloitte-france.fr/video/CPL/video.htm, durée : 4 min (consulté le 16.09.2013)

Annexe 1 : Canaux de communication proposés

Tableau des moyens d'information

Canaux	Explications	Avantages	Inconvénients
Information			
Direction de l'entreprise	Sensibiliser les membres de la direction afin qu'ils comprennent l'enjeu et l'importance d'un programme de sensibilisation de la sécurité de l'information. Demander leur soutien afin qu'ils communiquent directement avec leurs collaborateurs hiérarchiques et obtenir leur accord pour le financement du projet.	Par son engagement et son soutien dans le processus de sécurité, la direction montre que la sécurité est essentielle dans l'entreprise et leur accord pour le lancement du projet sera plus facile à obtenir.	Si la direction ne comprend pas l'importance d'un tel projet, il sera plus difficile de mettre un programme de sensibilisation en place.
Chef de groupe	Sensibiliser les cadres supérieurs sur l'importance de la sécurité et les grandes lignes de la politique de sécurité.	Ils communiqueront à leur groupe les principes de sécurité et feront donc office de relais pour rediffuser plus en profondeur dans la hiérarchie managériale du message de sensibilisation.	S'ils ne comprennent pas l'importance d'un tel projet, ils risquent d'être un frein à la propagation de l'information, voir même d'être les détracteurs du projet.
Règlement	Définir ces statuts généraux qui permettent d'expliquer ce qu'il doit être fait, afin de ne pas compromettre les quatre principaux fondements de la sécurité vus précédemment. Ainsi que les sanctions auxquels s'exposent les contrevenants.	Ce règlement permet de lister à un endroit les différents droits et devoirs des utilisateurs, et ainsi ils peuvent s'y référer en cas de doute.	Long et barbant généralement, il pourrait ne pas être lu ou tout du moins être survolé.
Charte informatique	Etablir un document qui explicite les droits et les devoirs des utilisateurs sur les ressources du système informatique. Elle doit être concise, lister les bonnes pratiques sécuritaires à mettre en place sur le système d'information et faire un rappel des interdictions, des restrictions, des obligations, résumer principes juridiques et les mesures de contrôle effectuées par l'entreprise.	Même principe que pour le règlement cela permet de lister à un endroit les différents droits et devoirs des utilisateurs, et ainsi ils peuvent s'y référer en cas de doute.	Elle pourrait ne pas être lue si elle est donnée avec d'autres documents à l'embauche de l'employé ou tout du moins être survolée.
Contrat	Emettre les grandes lignes de bonne conduite face au système d'information, afin qu'à la lecture le nouvel employé soit déjà informer du comportement à adopter.	Cela permet une entrée en matière en terme d'information pour le futur employé, ainsi il sait déjà à quoi s'en tenir.	Il pourrait ne pas le lire ou tout du moins le survoler.
Politique de sécurité	Elle permet de diffuser la vision de l'entreprise en matière de sécurité des systèmes d'information, établir la stratégie de sécurité et expliquer la bonne utilisation des outils du système d'information.	C'est un document qui reflète l'état d'esprit de la direction de l'entreprise, ainsi que de l'équipe de sécurité. Elle documente la culture de l'entreprise en matière de sécurité.	Elle pourrait ne pas être lue ou tout du moins être survolée.
Conférence	Mettre en place des réunions, conférences, ou séminaire portant sur la sécurité à l'intention des collaborateurs, permet de sensibiliser un groupe de personne sur la problématique de la sécurité en entreprise.	Elle permet de faire un premier pas en termes d'explications générales et de diffusion d'informations globalement importantes.	Comme les réunions ne touchent qu'un petit nombre de personne, il faudrait l'appliquer à un groupe bien déterminé pour avoir un impact stratégique.
Questionnaire	Fabriquer un questionnaire afin de permettre une évaluation des connaissances de chacun.	Cela permet de diffuser des informations de manière personnalisée et interactive.	Il se pourrait qu'il ne soit pas estimé à sa juste valeur, en étant trop vite rempli sans y prêter attention.

Tableau des moyens de communication

Canaux	Explications	Avantages	Inconvénients
Communication			
Site intranet	Communiquer les informations générales concernant la sécurité via un groupe de pages dédiées.	Cela permet d'avoir un endroit accessible à tous en tout temps où ils peuvent retrouver les diverses campagnes de sensibilisation, ainsi que des différents canaux de communication utilisés. Cela permet de diffuser les informations à tous les collaborateurs d'un coup et permet de centraliser de manière interne les informations dédiées à la sécurité.	L'utilisateur n'est pas obligé d'aller le consulté.
E-learning	Créer un site dédié ou le placer sur l'intranet, permet de regrouper toute l'information de sensibilisation et de faire un parcours personnalisé pour chaque employé.	Les utilisateurs peuvent s'informer de manière autonome. Ce qui permet un meilleur suivi de la sensibilisation de chacun et toucher tous les employés de l'entreprise.	L'utilisateur n'est pas obligé d'aller le consulté.
Réseau social d'entreprise	Utiliser un nouveau canal de diffusion afin de toucher les plus jeunes collaborateurs de l'entreprise.	C'est une façon innovante et actuelle de faire passer des messages courts et accrocheurs.	L'utilisateur n'est pas obligé d'aller le consulté. De plus, suivant l'utilisateur, il n'a pas l'habitude de vivre avec les réseaux sociaux.
Ecran de veille	Permet de faire passer des messages de sécurité visuelle ou textuelle aux utilisateurs, de manière personnalisée.	Si la communication est visuelle, elle facilite la compréhension des règles de sécurité, et c'est facile à mettre en place.	L'utilisateur peut supprimer les messages sans les avoir lu, ou tout simplement changer de fond d'écran ou d'écran de veille.
Fond d'écran			
Message sur l'ordinateur	Emettre un message à la connexion d'un utilisateur sur son poste de travail.	Il permet de cibler une catégorie d'employé et de personnaliser selon les besoins, le message de rappel.	L'utilisateur peut supprimer les messages sans les avoir lu.
Courrier électronique	Communiquer les règles générales de sécurité via le courrier électroniquepermetainsi de faireune campagne de prévention ou de rappel.	Il y a la possibilité de cibler les utilisateurs qui en ont besoin, ainsi que de personnaliser le message selon les catégories métiers de l'entreprise.	

Newsletter	Informe régulièrement tous les collaborateurs des règles générales de sécurité ou des mises à jour.	Il permet de faire des envois génaux, tout comme des envois ciblés à différentes catégories d'employés.	
SMS professionnel	Transmettre une alerte de sécurité via les téléphones professionnels est un bon moyen d'atteindre les employés.	Elle peut cibler tous les collaborateurs ou certaines catégories seulement et permet de rendre attentif en quelque seconde à une information importante.	Cependant, il faut que cette pratique soit gardée pour les cas d'importance majeure, sinon les employés risquent vite d'être agacés.
Affiches	Faire une campagne d'affichage dans l'entreprise permet de se faire une idée visuelle de la sécurité. Chaque affiche représente un ou plusieurs messages de manière imagée ou avec une petite phrase d'accroche. Ou répertorier sur un flyer toutes les informations utiles et visuelles.	Ce genre de support permet de faciliter la communication, et touche tous les employés en dehors de leur bureau de manière continue, comme dans les couloirs, les ascenseurs ou les salles de pause.	Ils peuvent vite s'en lasser, et ne plus les regarder. C'est pourquoi, il faut les renouveler après un certain laps de temps.
Brochure	Rendre les objets du quotidien professionnel porteurs de messages de sécurité. Utiliser des tasses, des verres, des portes clés, des fours d'ordinateurs, des clés USE, des tapis de souris ou des stylos pour véhiculer des petites phrases sécuritaires pense-bêtes.	Ce moyen permet de toucher de manière régulière et visuelle tous les employés, ainsi que de rendre itinérant le message à travers les gestes du quotidien.	Les employés risquent de s'en lasser, c'est pourquoi il faudrait renouveler les messages annuellement ou à l'occasion d'événements.
Objet quotidien	Créer une bande dessinée pour expliquer de manière ludique les usages sécuritaires des ressources du système d'information. Il n'y a pas besoin que soit sous forme d'une vrai bande dessinée papier, mais des petits encarts mis sur les écrans de veille, les fonds d'écran, les affiches, les flyers, dans les newsletters, sur les réseaux sociaux de l'entreprise, et centralisé sur l'intranet ou le e-learning.	Ce support permet de créer une image visuelle et explicite des comportements à adopter auprès de chaque employé. Cette manière de diffuser l'information sous forme humoristique permet de marquer l'esprit des collaborateurs.	Trop longue, elle pourrait être vite lassante. De plus, selon la manière dont elle est faite, elle peut ne pas intéresser.
Bande dessinée	Réaliser des vidéos et les mettre à disposition des employés via l'intranet ou le e-learning est une manière plus informelle et humoristique de faire passer des messages. Ces vidéos peuvent aussi tourner de manière régulière sur les écrans d'information de l'entreprise.	C'est une façon de toucher tous les collaborateurs et de leur permettre de visualiser les bonnes pratiques de sécurité.	L'utilisateur n'est pas obligé de la regarder, s'il veut la voir il est obligé de cliquer dessus. Elle peut être longue aussi, et vite lasser.
Vidéo			

Tableau des moyens de formation

Canaux	Explications	Avantages	Inconvénients
Formation			
Mise en situation	Former et sensibiliser les utilisateurs via des mises en situation réelle ou fictive permet d'impliquer d'une meilleure manière ceux-ci dans le processus de sécurité de l'entreprise.	Ceux-ci apprennent de manière interactive et proactive les usages sécuritaires du système d'information. L'être humain apprend mieux généralement quand il fait lui-même les actions, ce qui équivaut à créer l'expérience.	Les utilisateurs ne prendraient pas le temps de faire une formation, selon la charge de travail qu'ils ont.
Atelier	Organiser des ateliers pour des séances de formation de groupe avec un certain nombre d'utilisateurs ciblés où il sera proposé les divers travaux proposés dans ce chapitre comme les jeux, les questionnaires, basé sur des thèmes tirés du e-learning de l'entreprise.	Ces ateliers sont interactifs et permettent de donner plus d'impact à l'information diffusée.	Les utilisateurs ne prendraient pas le temps de faire une formation, selon la charge de travail qu'ils ont.
Coaching	Organiser des séances individuelle afin de former un collaborateur ayant plus de mal avec la sécurité au quotidien, ou tout simplement avec des utilisateurs qui doivent intégrer la sécurité dans leur gestes quotidiens par rapport à la sécurité.	Les séances de formation interne ou externe permettent de cibler par catégorie les utilisateurs, de personnaliser les travaux proposés, les canaux de communication à utiliser, les informations et les messages à diffuser auprès d'eux.	Les collaborateurs pourraient se sentir personnellement visés, et ne pas comprendre que ce n'est pas une sanction.
Formation externe	Ces formations données par d'autres entreprises ont le mérite d'être rodées, ce sont des professionnels dédiés qui les dispensent.		Elle coûte cher, bien qu'elle soit personnalisée aux besoins, ce n'est pas la même chose de faire une formation à l'extérieur, plutôt qu'à l'intérieur de l'entreprise où le collaborateur a ses marques.
Jeux	Jouer en groupe ou individuellement sur la sécurité des données et fabriquer des compétitions pour les collaborateurs, peut d'une certaine manière motiver les plus challengers. Le jeu permet aux utilisateurs de prendre conscience des problématiques, des solutions, de se poser les bonnes questions et d'apprendre sur la sécurité du système d'information.	Ce moyen interactif et original touche tous les collaborateurs, de manière personnalisée et permet l'apprentissage par l'expérience. Ces jeux peuvent être disponibles sur l'intranet ou lors des séances de formation individuelle ou de groupe.	Les utilisateurs ne prendraient pas le temps de faire une formation, selon la charge de travail qu'ils ont.

Annexe 2 : Mail de réponse

De : "X Commoy" <X.Commoy@terranovatraining.com>
Pour : "Borboën Claire-Stefanie (HES)" <claire-stefanie.borboen@etu.hesge.ch>
Objet : Formation Terranova inc. - Démonstration gratuite
Date : mar., sept. 17, 2013 16:28

Bonjour,
Je vous remercie de l'intérêt pour notre entreprise et produits.
Je regrette de vous informer que notre application est pour fin professionnelle.
Sincèrement,

Madame Commoy
Représentante aux ventes interne // Inside Sales
terranova
☎ 514.489.5806 | 1 866.889.5806 ext 208
✉ danielle.commoy@terranovatraining.com
www.formationterranova.com
www.terranovatraining.com

Annexe 3 : Interviews des entreprises privées

Situation :

Banque

Fonction/domaine: Administrateur système IT

Combien d'années au sein de l'entreprise : 2 ans

Questions :

1. **Avez-vous édicté une politique de sécurité (bonne conduite humaine) pour les utilisateurs concernant les systèmes d'information de votre entreprise?**

   Oui.

   1.1. **Sur quelle base l'avez-vous créée?**

   Sur des bases communes à tout type de plan de sécurité. Conseils de sécurité, normes, expériences.

   1.2. **De quelle manière, sous quelle forme?**

   Sous forme papier, sous forme orale et online.

   1.3. **Est-elle disponible à quelque part?**

   Oui. Sur l'intranet.

   1.4. **Cet endroit est-il connu des utilisateurs?**

   En théorie oui, cela devrait être connu, mais non, il ne pense pas que ce soit le cas.

   1.5. **Qui édicte ces règles de bonne conduite pour la sécurisation des données professionnelles ?**

   Une équipe chargée de la sécurité de l'information.

   1.6. **Diffusez-vous cette politique de sécurité?**

   Oui.

   1.6.1. **De quelle manière (moyens de communication, sous quelle forme)?**

   Programme pour les nouveaux employés avec environ 30 minutes d'explications lors de la présentation de l'entreprise.

   1.6.2. **A quelle fréquence?**

   Une fois à l'entrée de l'employé dans l'entreprise et ensuite quelques fois dans l'année.

   1.7. **Mettez-la vous à jour? A quelle fréquence?**

   Oui. Au gré de l'actualité et des audits faits par une entreprise externe et selon les besoins.

   1.8. **Avez-vous expliqué aux utilisateurs pourquoi ces règles sont importantes?**

   Oui.

   1.8.1. **Si oui, de quelle manière, sous quelle forme?**

   De manière électronique.

   1.8.2. **Pensez-vous qu'ils comprennent l'enjeu qui est derrière?**

   Non, pas toujours. Il y a une telle quantité de données traitées chaque jour, qu'à force ils ne font plus attention.

2. **Y-a-t-il une distinction qui est faite entre chaque domaine/département/poste pour la diffusion/communication de cette politique?**

   Oui. Il y a une base commune, mais quelques exceptions sont mises en place.

3. **Donnez-vous ou formez-vous un nouvel employé à se sensibiliser face aux risques de social engineering?**

Oui. Lors des séances d'introduction pour les nouveaux employés, des exemples sont donnés pour leur faire comprendre. Mais aussi aux autres employés lorsque c'est nécessaire.

4. Comptez-vous sur les utilisateurs pour qu'ils fassent attention ou restreignez-vous au maximum le risque d'incident avec les moyens dont vous disposez?

Nous restreignons un maximum les risques d'incidents grâce aux outils informatiques et électroniques. Nous ne laissons pas la responsabilité aux utilisateurs.

4.1. Pensez-vous que vous pourriez faire plus?

Oui, il y a toujours un potentiel d'amélioration.

4.2. Si oui, qu'est-ce qui vous en empêche?

Il s'agit des coûts que cela représente. Est-ce que cela vaut vraiment le cout ?

5. Prenez-vous des mesures envers les personnes qui auraient enfreint les règles?

Oui, cela dépend des cas.

5.1. De quels genres? Proportionnelles à l'importance de la fuite ou de la mise en danger potentielle des données?

Ca peut aller de l'avertissement au renvoi.

5.2. Si non, avez-vous planifié (envisagé car besoin) de les avoir un jour ?

-

6. Pour quelles raisons pensez-vous que les utilisateurs appliquent cette bonne *conduite ?*

Certains se sentent obligés, pour d'autres c'est par professionnalisme. Ils connaissent quand même que cela peut impactés leur travail.

6.1. Si oui pourquoi ?

✓ Ils comprennent les enjeux

✓ Ils se sentent contraints

❒ Ils le font parce qu'il faut le faire, sans forcément comprendre pourquoi

6.2. Si non pourquoi ?

✓ Oubli

❒ Ils ne comprennent pas pourquoi ils doivent faire attention

❒ Trop contraignant

❒ Ils ne les comprennent pas, donc ils ne peuvent pas les appliquer

7. Cette politique est-elle rediscutée à chaque mise à niveau budgétaire?

Oui, avec une équipe de la sécurité des SI.

8. Cette politique est-elle soumise aux restrictions budgétaires?

Cela se pourrait, mais n'est pas sur de connaitre la réponse.

9. Si vous deviez donner une note au résultat de votre travail de sensibilisation auprès des utilisateurs sur l'importance de la sécurité des données professionnelles, quelle serait-elle?

❒ 6 - Excellente

✓ 5 – Bonne

❒ 4- Suffisante

❒ 3- Insuffisante

❒ 2 – Echec

Situation :

Multinationale

Fonction/domaine: Superviseur du support IT

Combien d'années au sein de l'entreprise : en 2008 (5 ans)

Questions :

1. **Avez-vous édicté une politique de sécurité (bonne conduite humaine) pour les utilisateurs concernant les systèmes d'information de votre entreprise?**

   Oui. La Technology Gorvernance Risk and Controls User

   1.1. Sur quelle base l'avez-vous créée?

   Sur des bases communes à tout type de plan de sécurité.

   1.2. De quelle manière, sous quelle forme?

   Sous forme PDF, online.

   1.3. Est-elle disponible à quelque part?

   Oui. Sur l'intranet.

   1.4. Cet endroit est-il connu des utilisateurs?

   Non, il ne pense pas.

   1.5. Qui édicte ces règles de bonne conduite pour la sécurisation des données professionnelles ?

   Une équipe qui se nommait l'Information Protection. Maintenant c'est la Technology Gorvernance Risk and Controls User.

   1.6. Diffusez-vous cette politique de sécurité?

   Oui.

   1.6.1. De quelle manière (moyens de communication, sous quelle forme)?

   Mails, posters dans les lieux communs, programme pour les nouveaux employés avec environ 30 minutes d'explications lors de la présentation de l'entreprise.

   1.6.2. A quelle fréquence?

   Une fois à l'entrée de l'employé dans l'entreprise et ensuite quelques fois dans l'année.

   1.7. Mettez-la vous à jour? A quelle fréquence?

   Oui. Au gré de l'actualité et des audits faits par une entreprise externe et selon les besoins.

   1.8. Avez-vous expliqué aux utilisateurs pourquoi ces règles sont importantes?

   Oui.

   1.8.1. Si oui, de quelle manière, sous quelle forme?

   De manière verbale, par posters et par électronique.

   1.8.2. Si non pourquoi?

   -

   1.8.3. Pensez-vous qu'ils comprennent l'enjeu qui est derrière?

   Non, pas toujours. Ils veulent des outils faciles d'accès et accessibles rapidement, mais ils en oublient la sécurité-

2. **Y-a-t-il une distinction qui est faite entre chaque domaine/département/poste pour la diffusion/communication de cette politique?**

   Non. Elle est commune à tous. Mais il se peut qu'il y ait eu des particularités pour certains groupes d'employés.

3. **Donnez-vous ou formez-vous un nouvel employé à se sensibiliser face aux risques de social engineering?**

   Oui. Lors des séances d'introduction pour les nouveaux employés, des exemples sont donnés pour leur faire comprendre. Mais aussi aux autres employés lorsque c'est nécessaire.

4. **Comptez-vous sur les utilisateurs pour qu'ils fassent attention ou restreignez-vous au maximum le risque d'incident avec les moyens dont vous disposez?**

   Le minimum a été mis en place pour assurer une sécurité des données correctes.

   4.1. **Pensez-vous que vous pourriez faire plus?**

   Oui.

   4.2. **Si oui, qu'est-ce qui vous en empêche?**

   Il s'agit de faire la part des choses entre les risques réels et le business, il faut un équilibre entre les extrêmes pour que le business ne puisse pas être impacté par ces mesures.

5. **Prenez-vous des mesures envers les personnes qui auraient enfreint les règles?**

   Oui, cela dépend des cas.

   5.1. **De quels genres? Proportionnelles à l'importance de la fuite ou de la mise en danger potentielle des données?**

   Ca peut aller de l'avertissement au renvoi.

6. **Pour quelles raisons pensez-vous que les utilisateurs appliquent cette bonne *conduite* ?**

   Certains se sentent contraints, pour d'autres c'est par professionnalisme. Ils connaissent quand même que cela peut impactés leur travail. Pour d'autres c'est de la bonne conscience.

   6.1. **Si oui pourquoi ?**

   ✓ Ils comprennent les enjeux

   ✓ Ils se sentent contraints

   ❒ Ils le font parce qu'il faut le faire, sans forcément comprendre pourquoi

   6.2. **Si non pourquoi ?**

   ✓ Oubli

   ❒ Ils ne comprennent pas pourquoi ils doivent faire attention

   ❒ Trop contraignant

   ❒ Ils ne les comprennent pas, donc ils ne peuvent pas les appliquer

7. **Cette politique est-elle rediscutée à chaque mise à niveau budgétaire?**

   Oui, avec une équipe de la sécurité des SI.

8. **Cette politique est-elle soumise aux restrictions budgétaires?**

   Non, ou très peu.

9. **Si vous deviez donner une note au résultat de votre travail de sensibilisation auprès des utilisateurs sur l'importance de la sécurité des données professionnelles, quelle serait-elle? (en prenant en compte si cela a porté ces fruits)**

   ❒ 6 - Excellente

   ✓ 5 – Bonne

   ❒ 4- Suffisante

   ❒ 3- Insuffisante

   ❒ 2 – Echec

Situation :

PME

Fonction/domaine: Directeur du service IT interne

Combien d'années au sein de l'entreprise : environ 30 ans

Questions :

1. **Avez-vous édicté une politique de sécurité (bonne conduite humaine) pour les utilisateurs concernant les systèmes d'information de votre entreprise?**

   Oui.

   1.1. Sur quelle base l'avez-vous créée?

   Sur des bases communes à tout type de plan de sécurité. Conseils de sécurité, normes, expériences, conférences et MELANI.

   1.2. De quelle manière, sous quelle forme?

   Sous forme électronique.

   1.3. Est-elle disponible à quelque part?

   Oui, sur l'intranet. C'est le premier document que nous trouvons sur en première page.

   1.4. Cet endroit est-il connu des utilisateurs?

   Oui. Ils reçoivent d'ailleurs un courrier électronique leur rappelant où elle se trouve.

   1.5. Qui édicte ces règles de bonne conduite pour la sécurisation des données professionnelles ?

   Le service informatique interne avec la Direction.

   1.6. Diffusez-vous cette politique de sécurité?

   Oui. Un nouvel employé y est rendu attentif dès son engagement. Sinon, envoie de rappels quand il y a des changements.

   1.6.1. De quelle manière (moyens de communication, sous quelle forme)?

   Par rappels, explications, et séance de formation continue.

   1.6.2. A quelle fréquence?

   Une fois à l'entrée de l'employé dans l'entreprise et ensuite tous les deux mois.

   1.7. Mettez-la vous à jour? A quelle fréquence?

   Oui. En permanence.

   1.8. Avez-vous expliqué aux utilisateurs pourquoi ces règles sont importantes?

   Oui.

   1.8.1. Si oui, de quelle manière, sous quelle forme?

   De manière électronique et par des exemples concrets.

   1.8.2. Si non pourquoi?

   -

   1.8.3. Pensez-vous qu'ils comprennent l'enjeu qui est derrière?

   Oui et non. Ils estiment parfois que c'est exagéré.

2. **Y-a-t-il une distinction qui est faite entre chaque domaine/département/poste pour la diffusion/communication de cette politique?**

   Oui. Pour le domaine technique la sécurité est plus rigoureuse et régulière.

3. **Donnez-vous ou formez-vous un nouvel employé à se sensibiliser face aux risques de social engineering?**

   Non. Car dans l'entreprise tout le monde se connait.

4. **Comptez-vous sur les utilisateurs pour qu'ils fassent attention ou restreignez-vous au maximum le risque d'incident avec les moyens dont vous disposez?**

   Nous faisons les deux, afin que les mesures se complètent.

   4.1. **Pensez-vous que vous pourriez faire plus?**

   C'est déjà bien comme c'est actuellement, alors non nous ne pourrions pas faire plus.

5. **Prenez-vous des mesures envers les personnes qui auraient enfreint les règles?**

   Oui, cela dépend des cas.

   5.1. **De quels genres? Proportionnelles à l'importance de la fuite ou de la mise en danger potentielle des données?**

   Proportionnellement à l'incident commis.

6. **Pour quelles raisons pensez-vous que les utilisateurs appliquent cette *bonne conduite ?***

   6.1. **Si oui pourquoi ?**

   ✓ Ils comprennent les enjeux

   ✓ Ils se sentent contraints

   ✓ Ils le font parce qu'il faut le faire, sans forcément comprendre pourquoi

   6.2. **Si non pourquoi ?**

   ❒ Oubli

   ❒ Ils ne comprennent pas pourquoi ils doivent faire attention

   ❒ Trop contraignant

   ❒ Ils ne les comprennent pas, donc ils ne peuvent pas les appliquer

7. **Au niveau de la direction, est-ce facile de lui faire comprendre les enjeux et l'importance de cette sensibilisation (ex : moyens, temps et argent à prendre sur le temps de travail des utilisateurs) ?**

   Oui.

8. **Cette politique est-elle rediscutée à chaque mise à niveau budgétaire?**

   Non.

9. **Cette politique est-elle soumise aux restrictions budgétaires?**

   Non.

10. **Si vous deviez donner une note au résultat de votre travail de sensibilisation auprès des utilisateurs sur l'importance de la sécurité des données professionnelles, quelle serait-elle?**

   ❒ 6 - Excellente

   ✓ 5 – Bonne

   ❒ 4- Suffisante

   ❒ 3- Insuffisante

Il s'aperçoit que cela fonctionne, lorsque les utilisateurs lui posent des questions

Annexe 4 : Interviews à la Haute Ecole de Santé

Situation :

Haute Ecole de Santé (HEDS)

Fonction : Responsable informatique de la HEDS

Date de commencement dans cette école : 13 ans

Questions :

1. **Des règles de bonne conduite ont-elles été édictées pour la sécurisation des données professionnelles à la HEDS ?**

   Oui, de manière orale.

   1.1. Si oui, sur quoi sont-elles basées?

   Elles sont basées sur l'expérience et les informations lues dans les revues ou sites internet spécialisés ou transmises par les HES.

   1.1.1.Quand les transmettez-vous aux utilisateurs ?

   A l'engagement des employés.

   1.1.2.Pour quelles raisons selon-vous ces règles ont-elles été faites?

   Pour sensibiliser les utilisateurs à la manipulation de leur ordinateur.

2. **Pensez-vous que les utilisateurs sont aujourd'hui assez consciencieux pour qu'ils fassent attention sans qu'on leur explique?**

   Non. Il pense que la plupart ne font pas attention à leurs gestes quotidiens, mais qu'il en y a en quand même qui y sont sensibles.

3. **Qui édicte les règles de bonne conduite pour la sécurisation des données professionnelles à la HEDS ?**

   C'est le responsable informatique qui dirige une réunion avec les autres collaborateurs du centre informatique, afin d'édicter des règles ou des mises à jours auxquelles il faut faire attention.

   3.1. Qui est le propriétaire de ces règles ? (ex : Centre informatique, ou HES, Etat)

   Il y a une charte informatique et elle est faite par la Direction.

4. **Y-a-t-il une distinction qui est faite entre chaque domaine/département/poste à la HEDS pour la communication ou l'édition de ces règles ?**

   Il n'y a pas de différence faite entre les utilisateurs employés par la HEDS, mais par contre il y a une différence entre les employés et les étudiants.

   Cette différence porte sur le potentiel risque de perte de leurs données personnelles (travaux, mémoires, dossiers, projets, recherches) qui seraient enregistrées sur le bureau et non sur l'espace disque à leur nom. Il y a aussi le fait qu'ils doivent faire attention à leur clé USB, d'éviter une seule copie de leurs fichiers, et trouver un mot de passe adéquat pour leurs différents accès. Ceci est expliqué lors de 45 min en début de première année, par le centre informatique.

5. **Sont-elles disponibles à quelque part ?**

   Oui, sur l'intranet dans le système Qualité de la HES.

   5.1. Si oui, cet endroit est-il connu des utilisateurs ? Peuvent-ils y accéder avec/sans restriction ?

   Oui cet endroit est connu des employés, ils peuvent y accéder. Sauf les étudiants.

6. **Avez-vous expliqué pourquoi ces règles sont importantes?**

   Il espère que ce soit fait par les deux administrateurs systèmes lorsqu'il y a un nouvel employé.

   6.1. Si oui, de quelle manière, quelle communication?

   Cela est fait de manière orale.

7. **Avez-vous un processus de mise à jour ?**

   Oui, lors des réunions informatiques (voir question 3.)

   7.1. Si oui, tout les combien de temps ?

   Selon incident, ou information de la HES ou selon ce qui est lu dans les revues spécialisé IT.

8. **Sur quelle base mettez-vous à jour celles-ci ?**

   Voir question 8.

9. **Comptez-vous sur les utilisateurs pour qu'ils fassent attention, ou restreignez-vous le plus possible les éventuelles fuites, afin d'éviter un maximum d'incidents ? (*Donnez-vous la responsabilité de la sécurisation de ses données à l'utilisateur lui-même ou prenez-vous vous-même les choses en main en tenant compte du facteur humain (ingénieur social) dans votre politique de sécurité.)***

   Il compte sur la responsabilité des utilisateurs, afin d'éviter tout soucis. Ce n'est pas faute d'avoir essayer, mais le problème c'est que les utilisateurs ont râlé à cause du manque de disponibilité immédiat de leurs fichiers ou de leur ordinateur.

10. **Avez-vous mis en place un système qui permet de sécuriser les données professionnelles (travaux, examens, compte utilisateur, clés USB cryptées) des utilisateurs face aux éventuels petits malins, intrus, ou virus?**

    Il y a des serveurs mis à disposition afin de stocker les données dessus.

    Il y a une règle de verrouillage forcé de session qui a été mise en place. C'est-à-dire qu'elle se ferme automatiquement au bout de 15 minutes d'inactivité.

    Une session ne peut pas être ouverte sur plus d'un poste à la fois, sauf pour les administrateurs du centre informatique, pour éviter tout problème.

11. **Pour quelles raisons pensez-vous que les utilisateurs les appliquent-elles, ou pas?**

    Il y a ceux qui comprennent ce que cela implique et jouent le jeu. Il y a ceux qui n'y pense pas, et se disent « advienne que pourra » le centre informatique est là. Il pense que pour les étudiants, ce n'est pas certains, car ils y en a beaucoup qui viennent « pleurés » car ils ont perdus leur dossiers, mémoires en fermant leur session.

12. **Pensez-vous quelles sont suffisantes?**

    Ce n'est pas suffisant.

    12.1. Si non, que devriez-vous rajouter ou mettre en place afin de palier à ces lacunes?

    Un temps, il y avait un système qui avait été mis en place pour les étudiants qui permettait d'expliquer correctement chaque manipulation sécuritaire avec un ordinateur, mais cela prenait trop de temps. Avant c'était 3 heures, maintenant c'est plus que 45 min pour 60 groupes de 20 personnes.

13. **Lorsqu'une brèche est trouvée (par une personne de la HES ou lors d'un incident), faites-vous une analyse, avec prise de mesure telle que remise à jour des règles et campagne de communication ?**

    Oui voir question 3. Mais à sa connaissance, il n'y a pas eu d'incident, ni d'intrus quelconque qui a essayé d'obtenir des informations frauduleusement.

14. **Avez-vous testé grandeur nature si elles étaient bien appliquées ?**

    14.1. Si non, pour quelle raison ?

    Non, car il n'a pas le temps. Mais pensait faire disparaitre dans un dossier caché tous les fichiers du bureau d'un employé imprudent, afin de lui faire une frayeur. De cette manière, ce choque émotionnel, lui permettrait de lui faire comprendre l'importance de ne pas laisser sa session ouverte à tout les vents, ni même son bureau, et ensuite de mettre sur l'espace disque personnel ses documents afin qu'ils soient en sécurité.

Profil :

Masculin — Haute Ecole de Santé

Fonction, domaine : Directeur adjoint de la HEDS

Date de commencement dans cette école : 1 an

Questions :

1. Avez-vous reçu des règles de bonne conduite concernant la sécurité de vos données professionnelles de la part de l'école? (*Si oui, me donner un exemplaire*)

Oui et non. C'est-à-dire aucune directive venant de la direction HES. Mais sinon à son ancien poste ici, oui.

1.1. Si oui, de la part de qui ? (*ex : Centre Informatique, Direction, HES-GE principale*)

Direction de l'établissement.

1.1.1. Quand? (*ex : Chaque année, semestre, après incident*)

A l'engagement.

1.1.2. Comment, par quel(s) moyen(s) de communication?

Ecrite.

1.1.3. Avez-vous reçu des mises à jour ou des rappels, durant l'année, ou à chaque début d'année scolaire?

Oui.

1.2. Si non, pour quelle(s) raison(s) pensez-vous ?

Il n'y a pas de directives HES.

1.2.1. Faites-vous tout de même attention ?

Oui

1.2.2. Quelle(s) mesure(s) prenez-vous de votre propre initiative ?

Il fait attention à tout.

2. Vous a-t-on expliqué ces règles?

Non.

2.1. Si non, pour quelle(s) raison(s) pensez-vous ?

Un oubli.

3. Comprenez-vous pourquoi l'école édicte des règles à appliquer concernant la sécurité de vos données professionnelles ?

Oui.

3.1. Savez-vous les appliquer ?

Oui. De part son ancienne profession. Il travaillait aux assurances AI et ensuite aux Ressources Humaines de l'école.

3.2. Comprenez-vous exactement ce que chacune d'elle implique? (*me donner un exemple de règle incomprise, si la réponse est négative*)

Oui.

4. **Appliquez-vous ces directives totalement, partiellement, ou pas du tout ?**

   Totalement.

   4.1. Si oui, pour quelle(s) raison(s) ?

   ✓ Parce que vous avez compris exactement ce que cela implique.

   ❒ Plutôt par bonne conscience ou ne pas recevoir de remontrance.

   ❒ Autre :

   4.2. Si non, pour quelle(s) raison(s) ?

   ❒ Pas envie d'y penser.

   ❒ Trop contraignant.

   ❒ Parce que vous ne les comprenez pas.

   ❒ Vous les oubliez, tellement y en a.

5. **Que faites vous pour sécuriser vos données avec les outils informatiques quotidiens et dans le cadre général professionnel ?**

   Voir la question 1.2.2.

6. **Si une (nouvelle) campagne de communication concernant la sensibilisation à la sécurité de vos données professionnelles venait à se faire. Sous quelle forme souhaiteriez-vous qu'elle se face et pour quelle(s) raison(s)?**

   Une campagne visuelle, et une sensibilisation à l'arrivée d'un collaborateur, et il insiste sur ce fait.

7. **Pensez-vous que sous cette forme, vous seriez plus touché par ces bonnes pratiques?**

   Ce serait régulièrement vu, donc oui à force.

En tant que directeur adjoint :

1. **Comprenez-vous qu'une campagne de communication pour sensibiliser les employés à la sécurité des données de l'école, soit importante ?**

   Tout à fait.

2. **Avez-vous alloué un budget pour cette partie spécifique de la sécurité des informations au centre informatique ? Si ce n'est pas vous, qui c'est ?**

   Actuellement non. Mais s'il devait y avoir une campagne, il pourrait le faire. Car l'école est très en retard par rapport à ce qui est fait à l'Etat de Genève.

3. **Ce budget, serait-il sujet à une révision à la baisse en cas de crise financière ?**

   Oui, il pourrait.

4. **Pensez-vous que ce qui est fait actuellement est suffisant ?**

   Non.

5. **Demandez-vous au centre informatique de faire une mise à jour des informations ou de faire différemment, après un incident ?**

   Le service informatique le fait spontanément.

Profil :

Masculin — Haute Ecole de Santé

Fonction, domaine : Professeur en soins infirmiers à la HEDS

Date de commencement dans cette école :

Questions :

1. **Avez-vous reçu des règles de bonne conduite concernant la sécurité de vos données professionnelles de la part de l'école? (*Si oui, me donner un exemplaire*)**

   Oui. Mais il pense que les autres employés ont oubliés qu'il y a eu une campagne faite quand le directeur adjoint de l'actuelle Haute Ecole de Gestion était à la direction.

   1.1. **Si oui, de la part de qui ? (*ex : Centre Informatique, Direction, HES-GE principale*)**

   De la part du Centre Informatique et de la Direction antérieure à l'actuelle.

   1.1.1. **Quand? (*ex : Chaque année, semestre, après incident*)**

   En 2005.

   1.1.2. **Comment, par quel(s) moyen(s) de communication?**

   Il a reçu un mail, avec un mémo qui contenait ces bonnes pratiques.

   1.1.3. **Avez-vous reçu des mises à jour ou des rappels, durant l'année, ou à chaque début d'année scolaire?**

   Oui des rappels lors de nouveaux virus et incidents quelconques.

   1.1.4. **Pour quelle(s) raison(s), ou à quelle occasion?**

   Il a reçu ces bonnes pratiques à son engagement.

2. **Vous a-t-on expliqué ces règles?**

   Non.

   2.1. **Si non, pour quelle(s) raison(s) pensez-vous ?**

   Dans les informations reçues, il est indiqué qu'ils ont la possibilité de poser des questions s'il y en avait.

3. **Comprenez-vous pourquoi l'école édicte des règles à appliquer concernant la sécurité de vos données professionnelles ?**

   Oui.

   3.1. **Savez-vous les appliquer ?**

   Oui.

   3.2. **Comprenez-vous exactement ce que chacune d'elle implique? (*me donner un exemple de règle incomprise, si la réponse est négative*)**

   Oui.

4. **Appliquez-vous ces directives totalement, partiellement, ou pas du tout ?**

4.2. Si non, pour quelle(s) raison(s) ?

❒ Pas envie d'y penser.

❒ Trop contraignant.

❒ Parce que vous ne les comprenez pas.

❒ Vous les oubliez, tellement y en a.

5. Que faites vous pour sécuriser vos données avec les outils informatiques quotidiens et dans le cadre général professionnel ?

- *Il fait attention à tout, il lit tout ce qui lui est transmis.*
- *Il récupère les documents sensibles qui auraient pu rester dans la photocopieuse après un bourrage papier. Il fait attention aux virus, aux spams.*
- *Il verrouille sa session, ferme son bureau. Il ne donne pas d'information sans avoir demandé au préalable pourquoi.*
- *Il fait attention aux gens qui se trouvent dans les bureaux. Il ne met pas de clés USB inconnues dans son ordinateur.*
- *Il fait des sauvegardes de ses dossiers sur un disque dur externe.*

6. Si une (nouvelle) campagne de communication concernant la sensibilisation à la sécurité de vos données professionnelles venait à se faire. Sous quelle forme souhaiteriez-vous qu'elle se face et pour quelle(s) raison(s)?

Il verrait bien une ou plusieurs vidéos sympas qui représenteraient les gestes à faire au quotidien pour éviter de faire un faux pas. Il pense que des cours spécifiques d'une ou deux heures pourraient être bien, un mémo aussi afin de récapituler.

Il propose aussi une chambre virtuelle où un cours est dispensé à toute heure, afin de répondre aux questions ou une information qui tourne lorsqu'elle est demandée.

Il voit le jeu de rôles comme un bon moyens de faire comprendre aux employés qu'il y a toujours des failles dans leurs gestes quotidiens.

7. Pensez-vous que sous cette forme, vous seriez plus touché par ces bonnes pratiques?

Oui.

8. Pensez-vous que vous pourriez mieux les comprendre ou automatiser ces gestes au quotidien?

Oui.

Nos commentaires par rapport à l'entretien :

Il nous a expliqué aussi qu'il lisait tout ce que la direction envoyait, tous les mémos et autres communications des ressources humaines, et des autres départements. Il se renseigne sur tous les nouveaux employés, il voit leur visage dans AGE et connait dans la majorité des cas les bureaux de chacun. Mais qu'avec les changements de bureau fréquent en ce moment, il ne pourrait pas dire si certains sont encore au même endroit.

Ce qui soulève un point crucial : plus les gens changent de bureau, moins nous pouvons lutter contre d'éventuels « intrus », car nous ne sommes plus sûrs que les gens qui sont dans ce bureau sont bien ceux que nous voyons, si nous ne connaissons pas bien les nouveaux employés.

Profil :

Féminin — Haute Ecole de Santé

Fonction, domaine : Professeure en soins infirmiers à la HEDS

Date de commencement dans cette école : 15 ans.

Questions :

1. **Avez-vous reçu des règles de bonne conduite concernant la sécurité de vos données professionnelles de la part de l'école?**

   Non. Elle n'a pas pris connaissance de la charte informatique depuis plus de 10 ans.

   1.1. **Si oui, de la part de qui ? (*ex : Centre Informatique, Direction, HES-GE principale*)**

   Elle ne se souvient pas.

   1.1.1. **Quand? (*ex : Chaque année, semestre, après incident*)**

   Il y a 10 ans environ.

   1.1.2. **Comment, par quel(s) moyen(s) de communication?**

   Elle ne sait plus.

   1.1.3. **Avez-vous reçu des mises à jour ou des rappels, durant l'année, ou à chaque début d'année scolaire?**

   Elle ne sait pas.

   1.1.4. **Pour quelle(s) raison(s), ou à quelle occasion?**

   Aucune.

2. **Vous a-t-on expliqué ces règles?**

   Non.

   2.1. **Si non, pour quelle(s) raison(s) pensez-vous ?**

   Elle estime que c'est par logique, selon les us et les coutumes.

   2.2. **Faites-vous tout de même attention ?**

   Oui, elle met en place ce qu'elle sait.

3. **Comprenez-vous pourquoi l'école édicte des règles à appliquer concernant la sécurité de vos données professionnelles ?**

   Oui.

   3.1. **Savez-vous les appliquer ?**

   Oui.

   3.2. **Comprenez-vous exactement ce que chacune d'elle implique? (*me donner un exemple de règle incomprise, si la réponse est négative*)**

   Oui.

4. **Appliquez-vous ces directives totalement, partiellement, ou pas du tout ?**

Totalement.

4.1. Si oui, pour quelle(s) raison(s) ?

✓ Parce que vous avez compris exactement ce que cela implique.

❒ Plutôt par bonne conscience ou ne pas recevoir de remontrance.

❒ Autre :

4.2. Si non, pour quelle(s) raison(s) ?

❒ Pas envie d'y penser.

✓ Trop contraignant.

❒ Parce que vous ne les comprenez pas.

❒ Vous les oubliez, tellement y en a.

5. **Que faites vous pour sécuriser vos données avec les outils informatiques quotidiens et dans le cadre général professionnel ?**

- *Elle verrouille tout. Ex : casiers, session, portes.*

6. **Si une (nouvelle) campagne de communication concernant la sensibilisation à la sécurité de vos données professionnelles venait à se faire. Sous quelle forme souhaiteriez-vous qu'elle se face et pour quelle(s) raison(s)?**

Il faudrait qu'elle soit dynamique, interactive, sympathique, attrayante. Avec des supports tels que des vidéos, des slogans ou des petites bandes dessinées.

7. **Pensez-vous que sous cette forme, vous seriez plus touché par ces bonnes pratiques?**

Oui, elle pense qu'il y aurait plus d'impact.

8. **Pensez-vous que vous pourriez mieux les comprendre ou automatiser ces gestes au quotidien?**

Oui, et cela lui permettrait de ne pas avoir besoin de prendre connaissance du vocabulaire spécifique à l'informatique, car la campagne serait vulgarisée.

Nos commentaires par rapport à l'entretien :

Elle explique tout de même qu'elle ne consulte pas le service informatique pour installer des applications sur son ordinateur, car c'est trop long d'obtenir leur approbation.

Profil :

Masculin — Haute Ecole de Santé

Fonction, domaine : Professeur en soins infirmiers à la HEDS

Date de commencement dans cette école : 13 ans.

Questions :

1. **Avez-vous reçu des règles de bonne conduite concernant la sécurité de vos données professionnelles de la part de l'école? (*Si oui, me donner un exemplaire*)**

   Oui. Mais il pense que les autres employés ont oubliés qu'il y a eu une campagne faite quand le directeur adjoint de l'actuelle Haute Ecole de Gestion était à la direction.

   1.1. Si oui, de la part de qui ? (*ex : Centre Informatique, Direction, HES-GE principale*)

   De la part du Centre Informatique et de la Direction antérieure à l'actuelle.

   1.1.1. Quand? (*ex : Chaque année, semestre, après incident*)

   A son engagement, et en 2005.

   1.1.2. Comment, par quel(s) moyen(s) de communication?

   Durant une séance plénière avec tous les collaborateurs de l'époque.

   1.1.3. Avez-vous reçu des mises à jour ou des rappels, durant l'année, ou à chaque début d'année scolaire?

   Oui des rappels lors de nouveaux virus et incidents quelconques.

   1.1.4. Pour quelle(s) raison(s), ou à quelle occasion?

   Dans le cadre d'une petite sensibilisation.

2. **Vous a-t-on expliqué ces règles?**

   Non. Mais il s'informe auprès du service informatique quand il a des questions.

   2.1. Si non, pour quelle(s) raison(s) pensez-vous ?

   Dans les informations reçues, il est indiqué qu'ils ont la possibilité de poser des questions s'il y en avait.

3. **Comprenez-vous pourquoi l'école édicte des règles à appliquer concernant la sécurité de vos données professionnelles ?**

   Oui.

   3.1. Savez-vous les appliquer ?

   Oui.

   3.2. Comprenez-vous exactement ce que chacune d'elle implique? (*me donner un exemple de règle incomprise, si la réponse est négative*)

   Oui.

4. **Appliquez-vous ces directives totalement, partiellement, ou pas du tout ?**

Totalement.

4.1. Si oui, pour quelle(s) raison(s) ?

✓ Parce que vous avez compris exactement ce que cela implique.

❒ Plutôt par bonne conscience ou ne pas recevoir de remontrance.

❒ Autre :

4.2. Si non, pour quelle(s) raison(s) ?

❒ Pas envie d'y penser.

❒ Trop contraignant.

❒ Parce que vous ne les comprenez pas.

❒ Vous les oubliez, tellement y en a.

5. **Que faites vous pour sécuriser vos données avec les outils informatiques quotidiens et dans le cadre général professionnel ?**

- *Il fait attention à tout.*
- *Il verrouille tout. Ex : casiers, session, portes.*
- *Il ne transfère rien sur son téléphone portable.*
- *Il fait des sauvegardes de ses dossiers sur un disque dur externe.*

6. **Si une (nouvelle) campagne de communication concernant la sensibilisation à la sécurité de vos données professionnelles venait à se faire. Sous quelle forme souhaiteriez-vous qu'elle se face et pour quelle(s) raison(s)?**

Il avait apprécié que la première information ait été faite en séance plénière. Comme cela, les collaborateurs peuvent poser des questions et les règles sont explicitées.

7. **Pensez-vous que sous cette forme, vous seriez plus touché par ces bonnes pratiques?**

Oui.

8. **Pensez-vous que vous pourriez mieux les comprendre ou automatiser ces gestes au quotidien?**

Oui.

Nos commentaires par rapport à l'entretien :

C'est un collaborateur qui pose énormément de questions pour rester informé sur le sujet de l'informatique. Il a une très bonne prise de conscience de ce point de vue.

Profil :

Féminin — Haute Ecole de Santé

Fonction, domaine : Secrétaire au bureau des admissions

Date de commencement dans cette école : 1999 (14 ans)

Questions :

1. **Avez-vous reçu des règles de bonne conduite concernant la sécurité de vos données professionnelles de la part de l'école?**

   Oui, une charte informatique.

   1.1. **Si oui, de la part de qui ? (*ex : Centre Informatique, Direction, HES-GE principale*)**

   De la direction de la Haute Ecole de Santé.

   1.2. **Quand? (*ex : Chaque année, semestre, après incident*)**

   A son engagement dans l'école.

   1.3. **Comment, par quel(s) moyen(s) de communication?**

   Sur papier, dans le dossier donné à tous les nouveaux employés lors de l'engagement.

   1.4. **Avez-vous reçu des mises à jour ou des rappels, durant l'année, ou à chaque début d'année scolaire ?**

   Oui. Deux rappels.

   1.5. **Pour quelle(s) raison(s), ou à quelle occasion?**

   Une fois lors du changement de statut de l'école en HES et lors du changement de la messagerie sous Outlook.

   Sinon, une fois aussi quand la direction à rappeler que la messagerie devait être utilisé à des fins professionnelles, pour éviter les spams. A cause d'une invasion répétitive de spams qui auraient eu lieu.

2. **Vous a-t-on expliqué ces règles?**

   Non

   2.1. **Si non, pour quelle(s) raison(s) pensez-vous ?**

   Elle pense qu'ils n'y ont pas pensé, ou n'ont pas eu le temps de le faire. Mais surtout pour permettre un envoi multiple et perdre le moins de temps possible.

3. **Comprenez-vous pourquoi l'école édicte des règles à appliquer concernant la sécurité de vos données professionnelles ?**

   Oui

   3.1. **Savez-vous les appliquer ?**

   Oui. Applique celles dont elle se rappelle et sinon applique naturellement le secret de fonction.

   3.2. **Comprenez-vous exactement ce que chacune d'elle implique? (*me donner un exemple de règle incomprise, si la réponse est négative*)**

   Comme elle ne les a pas toutes lues, elle ne peut pas m'expliquer. Mais surtout elle ne se souvient pas exactement ce qui a été écrit.

4. **Appliquez-vous ces directives totalement, partiellement, ou pas du tout ?**

   Totalement.

4.1. **Si oui, pour quelle(s) raison(s) ?**

✓ Parce que vous avez compris exactement ce que cela implique.

❒ Plutôt par bonne conscience ou ne pas recevoir de remontrance.

❒ Autre :

4.2. **Si non, pour quelle(s) raison(s) ?**

❒ Pas envie d'y penser.

❒ Trop contraignant.

❒ Parce que vous ne les comprenez pas.

❒ Vous les oubliez, tellement y en a.

5. **Que faites vous pour sécuriser vos données avec les outils informatiques quotidiens et dans le cadre général professionnel ?**

- *Elle broie les papiers sensibles, récupère les papiers qui sont restés coincés dans l'imprimante. Mets tous documents professionnels sous clés.*
- *Elle ne communique absolument aucune donnée concernant par exemple un étudiant admis ou non tant que celui-ci n'a pas reçu de lettre officielle, même à un enseignant qui aurait sont enfant dans ce cas là.*
- *Elle évite de mettre à jour le statut de ce même étudiant dans AGE tant que lui-même n'a rien reçu, afin d'éviter qu'un parent enseignant à la HEDS puisse voir le statut dans AGE, avant confirmation officielle.*
- *Elle part du principe que toutes informations dites dans le bureau restent dans le bureau.*
- *Elle verrouille sa session, ne va pas sur les réseaux sociaux au bureau, efface tout courrier potentiellement dangereux à ses yeux.*

6. **Si une (nouvelle) campagne de communication concernant la sensibilisation à la sécurité de vos données professionnelles venait à se faire. Sous quelle forme souhaiteriez-vous qu'elle se face et pour quelle(s) raison(s)?**

Sous forme de courtes vidéos humoristiques ou sketch comme cela se fait parfois à la HEDS dans le cadre de la santé. Avec à la fin un résumé écrit, afin de pouvoir y jeter un œil si une fois elle ne se souvient plus.

7. **Pensez-vous que sous cette forme, vous seriez plus touché par ces bonnes pratiques?**

Oui, car c'est plus parlant pour elle comme cela, qu'une charte ou un mémo envoyé par mail.

8. **Pensez-vous que vous pourriez mieux les comprendre ou automatiser ces gestes au quotidien?**

Oui, car ce serait visuel et donc plus détaillé afin de faire passer le message.

Nos commentaires par rapport à l'entretien :

Elle m'avoue dès le départ, qu'elle pense avoir reçu ces informations, mais ne les a pas lu, car cela ne l'a pas intéressé de lire une page recto verso de chose à faire ou à ne pas faire.

Donc avec ça elle ne peut pas me dire ce qu'elle contenait, et ne sait pas où est-ce qu'elle pourrait les prendre pour me les donner.

Cela nous prouve que même si une charte informatique ou un document concernant la sensibilité des données était mise en place, ce ne serait pas seulement sous forme de papier. Car personne ne prend le temps de lire toute la paperasse donnée en début d'engagement, ou les mails envoyer dans le tas de ceux qui concernent le travail à accomplir durant la journée.

Elle nous fait part du fait qu'elle trouve insensé que les casiers soient ouverts à tout le monde dans un couloir principal. Tout le monde pourrait piocher pour voir ce qui se trouve dans les boîtes aux lettres de chacun, comme par exemple la direction, les ressources humaines ou les professeurs.

Situation :

Féminin — Haute Ecole de Santé

Fonction, domaine : Secrétaire au bureau des relations internationales

Date de commencement dans cette école : 2012 (1 année)

Questions :

1. **Avez-vous reçu des règles de bonne conduite concernant la sécurité de vos données professionnelles de la part de l'école?**

   D'abord elle a répondu non. Puis après réflexion, elle a dit oui, mais peu clair.

   1.1. **Si oui, de la part de qui ? (*ex : Centre Informatique, Direction, HES-GE principale*)**

   De la Direction de la HEDS

   1.1.1. **Quand? (*ex : Chaque année, semestre, après incident*)**

   A son engagement.

   1.1.2. **Comment, par quel(s) moyen(s) de communication?**

   Un papier qui concerne plus ou moins les devoirs et droits des employés dans le dossier d'engagement reçu le premier jour.

   1.1.1. **Avez-vous reçu des mises à jour ou des rappels, durant l'année, ou à chaque début d'année scolaire?**

   Non.

   1.2. **Si non, pour quelle(s) raison(s) pensez-vous ?**

   (En réponse au fait qu'elle les trouve peu claires étant donné qu'elle ne traite pas vraiment de bonnes pratiques informatiques.)

   Elle pense que c'est de la négligence de la part des responsables.

   1.2.1. **Faites-vous tout de même attention ?**

   Oui.

   1.2.2. **Quelle(s) mesure(s) prenez-vous de votre propre initiative ?**

   - *Elle verrouille sa session quand elle n'est pas au bureau.*
   - *Elle ferme sa porte à clés, lorsqu'elle sort du bureau.*
   - *Elle ne navigue sur aucun site qui n'a pas de rapport direct avec son travail.*
   - *Elle broie chaque document confidentiel. Elle utilise son ordinateur seulement à des fins professionnelles. Si elle veut consulter ses messages personnels, elle consulte son natel.*
   - *Elle ne transmet aucune information à des personnes ou collègues qui ne sont pas concernés.*

2. **Vous a-t-on expliqué ces règles?**

   Non.

   2.1. **Si non, pour quelle(s) raison(s) pensez-vous ?**

   Par négligence. Elle ne comprend pas pourquoi il n'y a pas eu plus d'information, car c'est quand même important.

3. **Comprenez-vous pourquoi l'école édicte des règles à appliquer concernant la sécurité de vos données professionnelles ?**

   3.1. **Savez-vous les appliquer ?**

   Elle applique ce qu'elle sait appliquer. C'est-à-dire ce qu'elle a appris dans son dernier emploi.

   3.2. **Comprenez-vous exactement ce que chacune d'elle implique?**

   Oui.

4. **Appliquez-vous ces directives totalement, partiellement, ou pas du tout ?**

   Totalement. Elle ne mélange pas le privé du professionnel et fait très attention.

   4.1. **Si oui, pour quelle(s) raison(s) ?**

   ✓ Parce que vous avez compris exactement ce que cela implique.

   ✓ Plutôt par bonne conscience ou ne pas recevoir de remontrance.

   ❒ Autre :

   4.2. **Si non, pour quelle(s) raison(s) ?**

   ❒ Pas envie d'y penser.

   ❒ Trop contraignant.

   ❒ Parce que vous ne les comprenez pas.

   ❒ Vous les oubliez, tellement y en a.

5. **Que faites vous pour sécuriser vos données avec les outils informatiques quotidiens et dans le cadre général professionnel ?**

   Voir la question 1.2.2.

   Elle utilise une clé USB, où elle enregistre toutes ses données professionnelles, afin d'éviter une nouvelle perte comme cela c'est passé à l'été 2012. Les serveurs de la HEDS se sont crachés et ils ont perdu une grande partie de leurs données.

6. **Si une (nouvelle) campagne de communication concernant la sensibilisation à la sécurité de vos données professionnelles venait à se faire. Sous quelle forme souhaiteriez-vous qu'elle se face et pour quelle(s) raison(s)?**

   Elle propose une mise en situation et trouver le bon comportement face à ces cas pratiques proposés. Sous forme de vidéos très brèves et questionnaires. Recevoir par mail une attestation qui prouve que l'on a compris les bonnes pratiques. Tout ça sur un support virtuel, tel qu'un site internet et que l'on peut passer quand on a veut durant une période déterminée. A renouveler annuellement et à refaire tant que le résultat n'est pas de 100%. La durée serait de 15 minutes maximum.

   Les jeux de rôles au sein de l'entreprise seraient une bonne idée. Il y aurait un groupe de personne qui serait désigné par la direction qui aurait pour mission de collecter un maximum d'information qu'ils ne sont pas censés avoir connaissance, pendant une journée.

   La charte ne serait pas utile, car elle ne la lirait pas. Ni une ou plusieurs vidéos humoristiques, car ce serait trop de temps pris sur le travail de la journée.

7. **Pensez-vous que sous cette forme, vous seriez plus touché par ces bonnes pratiques?**

   Oui, car cela nous implique personnellement.

8. **Pensez-vous que vous pourriez mieux les comprendre ou automatiser ces gestes au quotidien?**

   Oui, ce serait plus explicite sous cette forme.

Nos commentaires par rapport à l'entretien :

Cette dame a travaillé dans une entreprise de sécurité informatique concernant les finances. Elle a donc un passé qui lui a permis de connaitre d'appréhender la sécurité informatique et les manipulations sécuritaires à faire.

Cependant, elle pense que l'anti virus est un filet indestructible, ce qui peut être légitime. Parce que quand nous lui avons demandé si elle faisait attention avec les clés USB inconnues, elle m'a dit que cela ne lui serait pas venu à l'esprit de faire attention et de ne pas aller voir si elle trouverait le nom de la personne qui l'aurait perdu. Elle pense que puisque l'anti-virus est là, alors il n'y a pas de soucis. Quand nous entendons l'ancien responsable informatique de la HEG, dire qu'il ne veut pas mettre une clé USB inconnue dans son ordinateur de l'école nous perdons nous-mêmes confiance dans ce même anti-virus.

Elle nous a fait remarquer que les boites aux lettres sont une catastrophe, car ouvertes à tous.

Profil :

Féminin — Haute Ecole de Santé

Fonction, domaine : Secrétaire à la réception de l'école

Date de commencement dans cette école : 2012 (1 année)

Questions :

1. **Avez-vous reçu des règles de bonne conduite concernant la sécurité de vos données professionnelles de la part de l'école? (*Si oui, me donner un exemplaire*)**

   Non.

   1.1. Si non, pour quelle(s) raison(s) pensez-vous ?

   Elle pense que c'est un oubli de la part des ressources humaines.

   1.1.1. Faites-vous tout de même attention ?

   Elle fait attention du mieux qu'elle peut, selon ce qu'elle sait.

   1.1.2. Quelle(s) mesure(s) prenez-vous de votre propre initiative ?

   Ferme le bureau annexe à la réception lorsqu'elle s'en va de sa place.

   Demande la carte d'étudiant aux étudiants qui souhaitent une clé pour ouvrir une salle de cours.

   Quand un étudiant ou un professeur oublie du matériel personnel ailleurs qu'à l'école et qu'une personne s'annonce à la réception par téléphone ou en personne. Contacte elle-même cette personne, afin d'éviter de transmettre des informations personnelles à un inconnu.

   S'il s'agit de questions professionnelles, elle transmet l'appel aux ressources humaines.

2. **Vous a-t-on expliqué ces règles?**

   Non.

   2.1. Si non, pour quelle(s) raison(s) pensez-vous ?

   Elle pense que c'est un oubli de la part de la Direction de la HEDS.

3. **Comprenez-vous pourquoi l'école édicte des règles à appliquer concernant la sécurité de vos données professionnelles ?**

   Oui.

   3.1. Savez-vous les appliquer ?

   Non puisqu'elle ne sait pas ce qu'elle doit faire. Par contre, elle applique seulement ce qu'elle juge important pour la sécurité.

   3.2. Comprenez-vous exactement ce que chacune d'elle implique? (*me donner un exemple de règle incomprise, si la réponse est négative*)

   Oui pour ce qui est des règles générales de bonne jugeotes concernant la sécurité.

4. **Appliquez-vous ces directives totalement, partiellement, ou pas du tout ?**

Partiellement.

4.1. Si oui, pour quelle(s) raison(s) ?

❒ Parce que vous avez compris exactement ce que cela implique.

❒ Plutôt par bonne conscience ou ne pas recevoir de remontrance.

✓ Autre : Puisqu'elle n'a pas reçu ces informations, elle applique ce qu'elle juge bon.

4.2. Si non, pour quelle(s) raison(s) ?

❒ Pas envie d'y penser.

❒ Trop contraignant.

❒ Parce que vous ne les comprenez pas.

✓ Vous les oubliez, tellement y en a.

4.2.1. Que faudrait-il pour que vous les appliquiez quotidiennement ?

Elle souhaiterait un mémo récapitulatif et explicatif des bonnes pratiques à appliquer, afin qu'elle puisse l'avoir sous le nez et le faire correctement.

5. **Que faites vous pour sécuriser vos données avec les outils informatiques quotidiens et dans le cadre général professionnel ?**

Rien.

6. **Si une (nouvelle) campagne de communication concernant la sensibilisation à la sécurité de vos données professionnelles venait à se faire. Sous quelle forme souhaiteriez-vous qu'elle se face et pour quelle(s) raison(s)?**

Elle la verrait par la transmission d'un mémo de la Direction.

7. **Pensez-vous que sous cette forme, vous seriez plus touché par ces bonnes pratiques?**

Oui.

8. **Pensez-vous que vous pourriez mieux les comprendre ou automatiser ces gestes au quotidien?**

Oui.

Profil :

Féminin — Haute Ecole de Santé

Fonction, domaine : Assistante au bureau des Ressources Humaines

Date de commencement dans cette école : 8 ans

Questions :

1. **Avez-vous reçu des règles de bonne conduite concernant la sécurité de vos données professionnelles de la part de l'école? (*Si oui, me donner un exemplaire*)**

   Oui.

   1.1. Si oui, de la part de qui ? (*ex : Centre Informatique, Direction, HES-GE principale*)

   De la part de la Direction.

   1.1.1. Quand? (*ex : Chaque année, semestre, après incident*)

   Au moment de l'engagement et lors de l'entretien d'embauche.

   1.1.2. Comment, par quel(s) moyen(s) de communication?

   De façon orale.

   1.1.3. Avez-vous reçu des mises à jour ou des rappels, durant l'année, ou à chaque début d'année scolaire?

   Non

   1.1.4. Pour quelle(s) raison(s), ou à quelle occasion?

   Elle a reçu ces directives pour être sûre qu'elle avait bien compris que son poste demandait un respect scrupuleux du secret professionnel. Toute donnée étant confidentielle.

2. **Vous a-t-on expliqué ces règles?**

   Oui.

   2.1. Si oui, de quelle(s) manière(s) ? Par quel(s) moyen(s) de communication ?

   De manière orale, pour expliquer les bonnes pratiques à adopter face aux situations possibles.

3. **Comprenez-vous pourquoi l'école édicte des règles à appliquer concernant la sécurité de vos données professionnelles ?**

   Oui.

   3.1. Savez-vous les appliquer ?

   Oui pour les cas standards. Ensuite, selon son jugement professionnel, et selon la situation.

   3.2. Comprenez-vous exactement ce que chacune d'elle implique? (*me donner un exemple de règle incomprise, si la réponse est négative*)

   Oui.

4. **Appliquez-vous ces directives totalement, partiellement, ou pas du tout ?**

   Totalement.

4.1. **Si oui, pour quelle(s) raison(s) ?**

✓ Parce que vous avez compris exactement ce que cela implique.

✓ Plutôt par bonne conscience ou ne pas recevoir de remontrance.

❒ Autre :

4.2. **Si non, pour quelle(s) raison(s) ?**

❒ Pas envie d'y penser.

❒ Trop contraignant.

❒ Parce que vous ne les comprenez pas.

❒ Vous les oubliez, tellement y en a.

5. **Que faites vous pour sécuriser vos données avec les outils informatiques quotidiens et dans le cadre général professionnel ?**

Elle ne parle qu'aux personnes concernées par les informations qu'elle doit transmettre. Maintient la confidentialité des personnes, des données et autres informations lors des rendez-vous.

Elle verrouille sa session et ferme sa porte à chaque fois qu'elle part de son bureau. Il y a des armoires fermées à clés.

Lorsque que quelqu'un d'inconnu à l'entreprise demande des informations sur un employé, elle contacte cet employé afin d'avoir son accord pour transmettre les informations demandées.

Elle broie les documents confidentiels. Imprime énormément de documents à l'intérieur de son bureau.

6. **Si une (nouvelle) campagne de communication concernant la sensibilisation à la sécurité de vos données professionnelles venait à ce faire. Sous quelle forme souhaiteriez-vous qu'elle se face et pour quelle(s) raison(s)?**

Elle pense que sous forme de mémo avec un récapitulatif ainsi que les règles à appliquer, ce serait quelque chose qu'elle adopterait bien. Parce que cela lui permettrait de se rappeler en cas de doutes de pouvoir suivre la marche à suivre correctement. Elle pourrait mieux trier les données à garder et les autres.

7. **Pensez-vous que sous cette forme, vous seriez plus touché par ces bonnes pratiques?**

Oui. Cela lui permettrait d'avoir une explication claire de ce qu'elle doit faire ou ne pas faire dans tout les cas de figure qu'elle viendrait à traiter dans son travail.

8. **Pensez-vous que vous pourriez mieux les comprendre ou automatiser ces gestes au quotidien?**

Elle pense que ça l'aiderait énormément, mais que parfois, elle doit aussi faire appel à son jugement personnel pour appliquer un traitement professionnel dans certains cas, lorsque certaines données sont demandées.

Nos commentaires par rapport à l'entretien :

Elle nous parle plus des données professionnelles en générale que des données de la manipulation de son ordinateur. Ce qui est tout à fait naturelle étant donné qu'elle a un poste hautement sensible. C'est le poste où toutes les données concernant les employés sont stockées et traitées.

Annexe 5 : Interviews à la Haute Ecole de Gestion

Situation :

Haute Ecole de Gestion

Fonction : Responsable informatique de la HEG

Date de commencement dans cette école : en 2000 (13 ans)

Questions :

1. **Des règles de bonne conduite ont-elles été édictées pour la sécurisation des données professionnelles à la HEG ?**

   Non.

   1.1. Si non, pourquoi ?

   Ce n'était pas une priorité, pour l'ancien responsable, d'en avoir une.

2. **Pensez-vous que les utilisateurs sont aujourd'hui assez consciencieux pour qu'ils fassent attention sans qu'on leur explique?**

   Non. Ils manquent encore de sensibilisation. Exemple : Ils veulent tous l'installation de Dropbox sur leur poste pour partager leurs fichiers professionnels, mais cela est interdit par la loi suisse LIPAD (Administration Suisse). Car, mettre un fichier professionnel sur internet c'est le rendre disponible sur le domaine public et cette loi dit bien que tout fichier doit rester sur le territoire suisse. Et au vu de l'actualité concernant la surveillance des données par les Etats-Unis, cela revient à dire que ce n'est définitivement plus sûr.

3. **Qui édicte les règles de bonne conduite pour la sécurisation des données professionnelles à la HEG ?**

   Comme il n'y a pas de charte ou de règles de bonne conduite, nous posons la question concernant la charte informatique signée par les étudiants. La charte informatique rédigée pour les étudiants a été écrite par la Direction Générale et le service juridique de la HES Genève.

   3.1. Qui est le propriétaire de ces règles ? (ex : Centre informatique, ou HES, Etat)

   La Haute Ecole de Spécialisée de Genève.

4. **Y-a-t-il une distinction qui est faite entre chaque domaine/département/poste à la HEDS pour la communication ou l'édition de ces règles ?**

   Non. Mais s'il y en avait une qui devait être mise en place, il n'y aurait pas de distinction. Une charte commune suffirait.

5. **Sont-elles disponibles à quelque part ?**

   Sur l'intranet Qualité de la HES Genève.

   5.1. Si oui, cet endroit est-il connu des utilisateurs ? Peuvent-ils y accéder avec/sans restriction ?

   Pour ce qui est des étudiants, comme cela est écrit sur la charte signée à l'entrée en première année, ils devraient le savoir.

6. **Si non, pour quelle raison ?**

   Mais pour ce qui est du personnel de la HEG, il ne pense pas que cela soit connu des utilisateurs, car depuis qu'ils n'ont plus besoin de la signer, ils ne se demandent plus où il pourrait la trouver.

7. **Avez-vous expliqué pourquoi ces règles sont importantes?**

   Sporadiquement, quand un utilisateur pose la question. Sinon.

7.1. Si non, pour quelle raison?

Parce qu'il n'y a pas de Politique de Sécurité. Pour pouvoir expliquer ces règles, il faudrait un plan.

8. Avez-vous un processus de mise à jour ?

Oui, il y en aurait un, si cela existait.

8.1. Si oui, tout les combien de temps ?

Ce serait au gré de l'actualité.

9. Sur quelle base mettez-vous à jour celles-ci ?

Ce serait en réaction à des incidents, ou en prévention par rapport à ce qui est lu et entendu dans la presse ou sites internet spécialisés.

10. Comptez-vous sur les utilisateurs pour qu'ils fassent attention, ou restreignez-vous le plus possible les éventuelles fuites, afin d'éviter un maximum d'incidents ? (*Donnez-vous la responsabilité de la sécurisation de ses données à l'utilisateur lui-même ou prenez-vous vous-même les choses en main en tenant compte du facteur humain (ingénieur social) dans votre politique de sécurité.)*

Il compte sur les utilisateurs pour qu'ils fassent attention. Le centre informatique a mis un place un système adapté pour sécuriser les données de chaque groupe d'utilisateurs (professeurs, administratifs, étudiants) afin d'éviter d'éventuels incidents (ex : session admin commune à utiliser pour les classes). Mais il y a toujours le risque humain qui n'est pas contrôlable.

11. Avez-vous mis en place un système qui permet de sécuriser les données professionnelles (travaux, examens, compte utilisateur, clés USB cryptées) des utilisateurs face aux éventuels petits malins, intrus, ou virus?

Par exemple, il a mis en place un serveur sécurisé avec mot de passe pour la création d'examens, où il est possible de déposer les fichiers, les lire et il est impossible de les déplacés ailleurs.

12. Pour quelles raisons pensez-vous que les utilisateurs les appliquent-elles, ou pas?

C'est une question d'information, de communication, de sensibilisation.

13. Pensez-vous quelles sont suffisantes?

Non.

13.1. Si non, que devriez-vous rajouter ou mettre en place afin de palier à ces lacunes?

Un plan de sécurité.

14. Lorsqu'une brèche est trouvée (par une personne de la HES ou lors d'un incident), faites-vous une analyse, avec prise de mesure telle que remise à jour des règles et campagne de communication ?

Il a fait un mail de prévention dernièrement contre le phishing, qu'il a transmis aux collaborateurs de la HEG et à ses autres collègues dans les autres HES. Sinon, il y a eu des mémos après les incidents qui correspondent à de la « guérison ».

15. Avez-vous testé grandeur nature si elles étaient bien appliquées ?

Non.

15.1. Si non, pour quelle raison ?

Il n'y a pas pensé.

Profil :

Masculin — Haute Ecole de Gestion

Fonction, domaine : Directeur adjoint de la HEG

Date de commencement dans cette école : 3 ans

Questions :

1. **Avez-vous reçu des règles de bonne conduite concernant la sécurité de vos données professionnelles de la part de l'école? (*Si oui, me donner un exemplaire*)**

   Il n'y a pas de procédure officielle, ce sont les uses et coutumes qui sont à utiliser.

   1.1. Si oui, de la part de qui ? (*ex : Centre Informatique, Direction, HES-GE principale*)

   Ce serait un mélange de la Direction et du Centre Informatique et de la Communication, si un récapitulatif venait à se mettre en place.

   1.1.1. Quand? (*ex : Chaque année, semestre, après incident*)

   Ce serait tout au début de l'année et de l'engagement des employés.

   1.1.2. Comment, par quel(s) moyen(s) de communication?

   Oralement, peut-être un document si vraiment c'est nécessaire.

   1.1.3. Avez-vous reçu des mises à jour ou des rappels, durant l'année, ou à chaque début d'année scolaire?

   Non. Mais s'il venait à y en avoir une serait appliquer dans le cadre Qualité, et il y aurait un processus d'audit avec ou non une mise à jour tous les 18 mois.

   1.1.4. Pour quelle(s) raison(s), ou à quelle occasion?

   Il compte en toucher un mot lors de la réunion de présentation pour les nouveaux employés de la HEG en août.

   1.2. Si non, pour quelle(s) raison(s) pensez-vous ?

   Car, « on compte sur les us et coutumes des employés »

   1.2.1. Faites-vous tout de même attention ?

   Personnellement, il fait attention, mais se rend compte qu'il y a encore des failles.

   1.2.2. Quelle(s) mesure(s) prenez-vous de votre propre initiative ?

   Il verrouille sa session, ferme son bureau, cache la vue de sa webcam. Utilise son ordinateur à des fins professionnelles. Ne met pas de clés USB inconnues dans son ordinateur. Utilise un disque dur pour sauvegarder des données.

2. **Vous a-t-on expliqué ces règles?**

   Il les a déterminées personnellement.

3. **Comprenez-vous pourquoi l'école édicte des règles à appliquer concernant la sécurité de vos données professionnelles ?**

   Oui.

   3.1. Savez-vous les appliquer ?

   Oui.

   3.2. Comprenez-vous exactement ce que chacune d'elle implique? (*me donner un exemple de règle incomprise, si la réponse est négative*)

   Oui.

4. **Appliquez-vous ces directives totalement, partiellement, ou pas du tout ?**

   Totalement.

   4.1. Si oui, pour quelle(s) raison(s) ?

   ✓ Parce que vous avez compris exactement ce que cela implique.

   ❒ Plutôt par bonne conscience ou ne pas recevoir de remontrance.

   ❒ Autre :

   4.2. Si non, pour quelle(s) raison(s) ?

   ❒ Pas envie d'y penser.

   ❒ Trop contraignant.

   ❒ Parce que vous ne les comprenez pas.

   ❒ Vous les oubliez, tellement y en a.

5. **Que faites vous pour sécuriser vos données avec les outils informatiques quotidiens et dans le cadre général professionnel ?**

   Voir la question 1.2.2.

6. **Si une (nouvelle) campagne de communication concernant la sensibilisation à la sécurité de vos données professionnelles venait à se faire. Sous quelle forme souhaiteriez-vous qu'elle se face et pour quelle(s) raison(s)?**

   Il faudrait qu'il se réunisse avec la communication et le centre informatique pour en discuter.

7. **Pensez-vous que sous cette forme, vous seriez plus touché par ces bonnes pratiques?**

   A voir selon ce qui est mis en place.

En tant que directeur adjoint :

1. **Comprenez-vous qu'une campagne de communication pour sensibiliser les employés à la sécurité des données de l'école, soit importante ?**

   Oui.

2. **Avez-vous alloué un budget pour cette partie spécifique de la sécurité des informations au centre informatique ? Si ce n'est pas vous, qui c'est ?**

   Non. Mais s'il devait y avoir une campagne, il pourrait le faire.

3. **Ce budget, serait-il sujet à une révision à la baisse en cas de crise financière ?**

   Oui, il pourrait.

4. **Pensez-vous que ce qui est fait actuellement est suffisant ?**

   Il pense qu'au niveau de l'infrastructure informatique cela est excellent, mais qu'au niveau humain, il reste des choses à faire.

5. **Demandez-vous au centre informatique de faire une mise à jour des informations ou de faire différemment, après un incident ?**

   Il demande une prise de mesure afin d'éviter un nouvel incident.

Profil :

Féminin — Haute Ecole de Gestion

Fonction, domaine : Secrétaire pour la formation continue

Date de commencement dans cette école : 10 ans.

Questions :

1. **Avez-vous reçu des règles de bonne conduite concernant la sécurité de vos données professionnelles de la part de l'école? (*Si oui, me donner un exemplaire*)**

   Oui. Une charte informatique, ainsi qu'un guide pour l'employé.

   1.1. Si oui, de la part de qui ? (*ex : Centre Informatique, Direction, HES-GE principale*)

   Des ressources humaines.

   1.1.1. Quand? (*ex : Chaque année, semestre, après incident*)

   A son engagement.

   1.1.2. Comment, par quel(s) moyen(s) de communication?

   Oral.

   1.1.3. Avez-vous reçu des mises à jour ou des rappels, durant l'année, ou à chaque début d'année scolaire?

   Non.

2. **Vous a-t-on expliqué ces règles?**

   Non. Mais elle s'informe auprès du service informatique quand elle a des questions.

   2.1. Si non, pour quelle(s) raison(s) pensez-vous ?

   Dans les informations reçues, il est indiqué qu'ils ont la possibilité de poser des questions s'il y en avait.

3. **Comprenez-vous pourquoi l'école édicte des règles à appliquer concernant la sécurité de vos données professionnelles ?**

   Oui.

   3.1. Savez-vous les appliquer ?

   Oui.

   3.2. Comprenez-vous exactement ce que chacune d'elle implique? (*me donner un exemple de règle incomprise, si la réponse est négative*)

   Oui. Si elle ne les comprend pas, elle pose des questions.

4. **Appliquez-vous ces directives totalement, partiellement, ou pas du tout ?**

Totalement.

4.1. Si oui, pour quelle(s) raison(s) ?

✓ Parce que vous avez compris exactement ce que cela implique.

❒ Plutôt par bonne conscience ou ne pas recevoir de remontrance.

❒ Autre :

4.2. Si non, pour quelle(s) raison(s) ?

❒ Pas envie d'y penser.

❒ Trop contraignant.

❒ Parce que vous ne les comprenez pas.

❒ Vous les oubliez, tellement y en a.

5. **Que faites vous pour sécuriser vos données avec les outils informatiques quotidiens et dans le cadre général professionnel ?**

Elle applique la sécurité de base, elle verrouille la porte du bureau, sa session et les tiroirs.

6. **Si une (nouvelle) campagne de communication concernant la sensibilisation à la sécurité de vos données professionnelles venait à se faire. Sous quelle forme souhaiteriez-vous qu'elle se face et pour quelle(s) raison(s)?**

Un récapitulatif des bonnes pratiques ce serait intéressant pour se remémorer ce qu'il doit être fait ou non. Mais surtout elle pourrait le stocker et le relire si un jour elle a un doute.

7. **Pensez-vous que sous cette forme, vous seriez plus touché par ces bonnes pratiques?**

Oui.

8. **Pensez-vous que vous pourriez mieux les comprendre ou automatiser ces gestes au quotidien?**

Oui. Il faudrait que ce récapitulatif soit aussi explicite qu'un cours de bureautique, avec par exemple des captures d'écran.

Profil :

Féminin — Haute Ecole de Gestion

Fonction, domaine : Professeure de communication et de comptabilité

Date de commencement dans cette école : 2011 (2 ans)

Questions :

1. **Avez-vous reçu des règles de bonne conduite concernant la sécurité de vos données professionnelles de la part de l'école? (*Si oui, me donner un exemplaire*)**

   Non.

   1.1. **Si non, pour quelle(s) raison(s) pensez-vous ?**

   Elle suppose que c'est parce que la direction (ou le service informatique) a estimé qu'elle saurait le faire toute seule. Pour elle, ils estiment que ça coule de source. (Corrobore ce que le directeur adjoint de cette école a dit.)

   1.1.1. **Faites-vous tout de même attention ?**

   Oui.

   1.1.2. **Quelle(s) mesure(s) prenez-vous de votre propre initiative ?**

   - *Elle verrouille sa session.*
   - *Elle ferme à clé le bureau.*

2. **Vous a-t-on expliqué ces règles?**

   Oui, quand elle pose la question.

   2.1. **Si oui, de quelle(s) manière(s) ? Par quel(s) moyen(s) de communication ?**

   Les explications lui parviennent de manière orale.

3. **Comprenez-vous pourquoi l'école édicte des règles à appliquer concernant la sécurité de vos données professionnelles ?**

   Oui.

   3.1. **Savez-vous les appliquer ?**

   Oui. Grâce aux collègues qui l'ont aidée.

   3.2. **Comprenez-vous exactement ce que chacune d'elle implique? (*me donner un exemple de règle incomprise, si la réponse est négative*)**

   Oui.

4. **Appliquez-vous ces directives totalement, partiellement, ou pas du tout ?**

Totalement.

4.1. Si oui, pour quelle(s) raison(s) ?

✓ Parce que vous avez compris exactement ce que cela implique.

❒ Plutôt par bonne conscience ou ne pas recevoir de remontrance.

❒ Autre :

4.2. Si non, pour quelle(s) raison(s) ?

❒ Pas envie d'y penser.

❒ Trop contraignant.

❒ Parce que vous ne les comprenez pas.

❒ Vous les oubliez, tellement y en a.

5. **Que faites vous pour sécuriser vos données avec les outils informatiques quotidiens et dans le cadre général professionnel ?**

Voir questions 1.1.2.

6. **Si une (nouvelle) campagne de communication concernant la sensibilisation à la sécurité de vos données professionnelles venait à se faire. Sous quelle forme souhaiteriez-vous qu'elle se face et pour quelle(s) raison(s)?**

Avec des affiches, des messages (type slogan) lisibles et immédiat. Il faudrait que les risques soient exemplifiés. Elle explique qu'une affiche est obligée d'être vue, car elle nous apparait sous les yeux, alors qu'une vidéo non. Pour la vidéo, elle est regardée de manière délibérée, donc moins visibles.

7. **Pensez-vous que sous cette forme, vous seriez plus touché par ces bonnes pratiques?**

Oui.

8. **Pensez-vous que vous pourriez mieux les comprendre ou automatiser ces gestes au quotidien?**

Oui.

Profil :

Masculin — Haute Ecole de Gestion

Fonction, domaine : Professeur de communication

Date de commencement dans cette école : 2003 (10 ans).

Questions :

1. **Avez-vous reçu des règles de bonne conduite concernant la sécurité de vos données professionnelles de la part de l'école? (*Si oui, me donner un exemplaire*)**

   Non.

   1.1. Si non, pour quelle(s) raison(s) pensez-vous ?

   Il pense que c'est un manque de ressources humaines, d'organisation, qu'ils sont plus axés sur l'essentiel.

   1.1.1. Faites-vous tout de même attention ?

   Oui, sans être parano non plus.

   1.1.2. Quelle(s) mesure(s) prenez-vous de votre propre initiative ?

   - Il ne prend jamais de clés USB, disque dur ou autres matériels pouvant être perdus ou volés dans la classe.
   - Il verrouille sa session tout le temps, tant dans une classe que dans le bureau.
   - Il met ses examens en lieu sûr dans sa session. Les élèves devraient « se lever tôt » pour les trouver s'ils venaient à accéder à sa session.
   - Il n'utilise pas les réseaux sociaux, il ne veut pas que des photos soient prises en classe, si un étudiant enregistre il souhaite être informé afin de donner son accord. Ces enregistrements sont « privés » à la classe, et ne doivent pas être sorti de leur contexte.

2. **Vous a-t-on expliqué ces règles?**

   Non, sauf lorsque qu'il y a des rappels.

   2.1. Si oui, de quelle(s) manière(s) ? Par quel(s) moyen(s) de communication ?

   Il a reçu des rappels, après des incidents, ou quand il y a des nouveaux virus, par mail sous forme de mémo.

3. **Comprenez-vous pourquoi l'école édicte des règles à appliquer concernant la sécurité de vos données professionnelles ?**

   Oui.

   3.1. Savez-vous les appliquer ?

   Oui. Il le fait quoiqu'il en soit, car il le faut.

   3.2. Comprenez-vous exactement ce que chacune d'elle implique? (*me donner un exemple de règle incomprise, si la réponse est négative*)

   Oui.

4. **Appliquez-vous ces directives totalement, partiellement, ou pas du tout ?**

   Totalement.

   4.1. Si oui, pour quelle(s) raison(s) ?

   ✓ Parce que vous avez compris exactement ce que cela implique.

   ❒ Plutôt par bonne conscience ou ne pas recevoir de remontrance.

   ✓ Autre : Par habitude.

   4.2. Si non, pour quelle(s) raison(s) ?

   ❒ Pas envie d'y penser.

   ❒ Trop contraignant.

   ❒ Parce que vous ne les comprenez pas.

   ❒ Vous les oubliez, tellement y en a.

5. **Que faites vous pour sécuriser vos données avec les outils informatiques quotidiens et dans le cadre général professionnel ?**

   Voir question 1.2.2.

6. **Si une (nouvelle) campagne de communication concernant la sensibilisation à la sécurité de vos données professionnelles venait à se faire. Sous quelle forme souhaiteriez-vous qu'elle se face et pour quelle(s) raison(s)?**

   Il verrait bien une vidéo décalée, humoristique qui montre les bonnes pratiques à mettre en place au quotidien.

7. **Pensez-vous que sous cette forme, vous seriez plus touché par ces bonnes pratiques?**

   Oui.

8. **Pensez-vous que vous pourriez mieux les comprendre ou automatiser ces gestes au quotidien?**

   Oui. Bien qu'il le fasse déjà.

   Nos commentaires par rapport à l'entretien :

   Ce monsieur est politicien, donc il a une vision de la sécurité des données déjà bien développée. Ce qui prouve pourquoi il ne souhaite pas que des photos de lui circulent, et encore moins des phrases dites lors de son cours sorties de son contexte.

Profil :

Féminin — Haute Ecole de Gestion

Fonction, domaine : Secrétaire de filière IG

Date de commencement dans cette école : 2011 (2 ans)

Questions :

1. **Avez-vous reçu des règles de bonne conduite concernant la sécurité de vos données professionnelles de la part de l'école? (*Si oui, me donner un exemplaire*)**

   Ne se souvient pas. Pense que cela à dû passer à la trappe avec toute la paperasse donnée à l'engagement.

   1.1. Si non, pour quelle(s) raison(s) pensez-vous ?

   -

   1.1.1. Faites-vous tout de même attention ?

   Oui.

   1.1.2. Quelle(s) mesure(s) prenez-vous de votre propre initiative ?

   Verrouille sa session (a appris à le faire seulement 2 mois après être engagée), ferme à clé le bureau, restreint les accès aux informations aux étudiants qui passent dans le bureau.

2. **Vous a-t-on expliqué ces règles?**

   Non pas de la part des personnes qui auraient dû le faire.

   2.1. Si oui, de quelle(s) manière(s) ? Par quel(s) moyen(s) de communication ?

   Mais oui lorsqu'elle a commencé au poste de secrétaire de filière. Elle apprit les gestes sécuritaires avec son ordinateur grâce à son chef.

   2.2. Si non, pour quelle(s) raison(s) pensez-vous ?

   Négligence.

3. **Comprenez-vous pourquoi l'école édicte des règles à appliquer concernant la sécurité de vos données professionnelles ?**

   Oui.

   3.1. Savez-vous les appliquer ?

   Maintenant oui.

   3.2. Comprenez-vous exactement ce que chacune d'elle implique? (*me donner un exemple de règle incomprise, si la réponse est négative*)

   Oui. Grâce aux collègues qui l'ont aidée.

4. **Appliquez-vous ces directives totalement, partiellement, ou pas du tout ?**

Totalement.

4.1. Si oui, pour quelle(s) raison(s) ?

✓ Parce que vous avez compris exactement ce que cela implique.

❒ Plutôt par bonne conscience ou ne pas recevoir de remontrance.

❒ Autre :

4.2. Si non, pour quelle(s) raison(s) ?

❒ Pas envie d'y penser.

❒ Trop contraignant.

❒ Parce que vous ne les comprenez pas.

❒ Vous les oubliez, tellement y en a.

5. **Que faites vous pour sécuriser vos données avec les outils informatiques quotidiens et dans le cadre général professionnel ?**

Voir questions 1.2.2.

6. **Si une (nouvelle) campagne de communication concernant la sensibilisation à la sécurité de vos données professionnelles venait à se faire. Sous quelle forme souhaiteriez-vous qu'elle se face et pour quelle(s) raison(s)?**

Une formation interactive, avec des vidéos, une recherche. Quelque chose qui bouge, qui implique l'utilisateur. Pas de charte ou de mémo ou de présentation d'une heure collée au siège en attendant que ce soit fini.

7. **Pensez-vous que sous cette forme, vous seriez plus touché par ces bonnes pratiques?**

Oui.

8. **Pensez-vous que vous pourriez mieux les comprendre ou automatiser ces gestes au quotidien?**

Oui.

Annexe 6 : Plan – Phase 1 - Planification

Phase 1

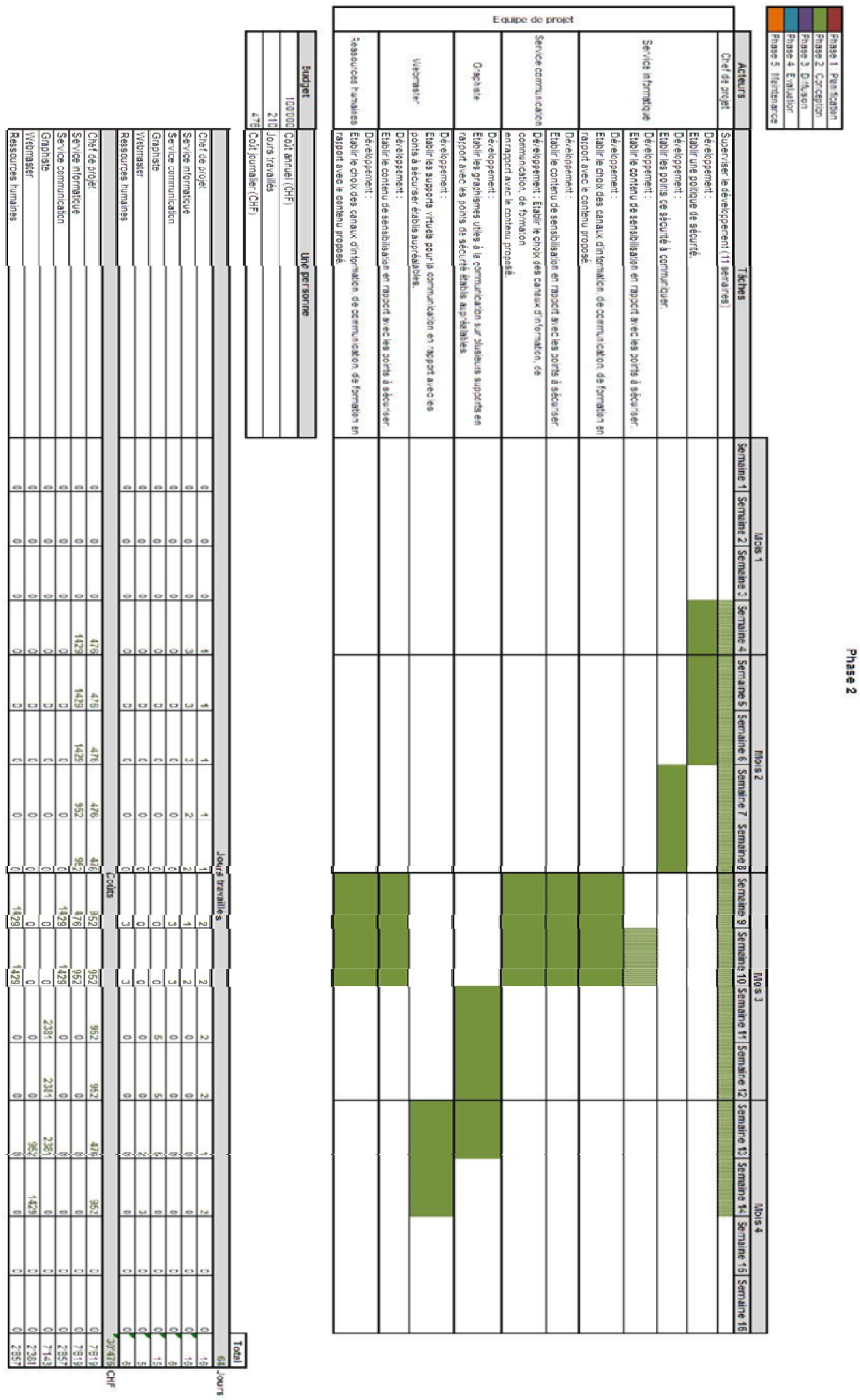
Phase 1 : Planification
Phase 2 : Conception
Phase 3 : Diffusion
Phase 4 : Evaluation
Phase 5 : Maintenance

			Mois 1			
	Acteurs	Tâches	Semaine 1	Semaine 2	Semaine 3	Semaine 4
Equipe de projet	Chef de projet	Planification : Préparer le projet de				
		Planification : Réunir la direction de				
		Planification : Réunir l'équipe de projet.				
	Service informatique	Planification : Réunion de l'équipe de projet.				
	Service communication	Planification : Réunion de l'équipe de projet.				
	Graphiste	Planification : Réunion de l'équipe de projet.				
	Webmaster	Planification : Réunion de l'équipe de projet.				
	Ressources humaines	Planification : Réunion de l'équipe de projet.				

Budget	Une personne
100'000	Coût annuel (CHF)
210	Jours travaillés
476	Coût journalier (CHF)

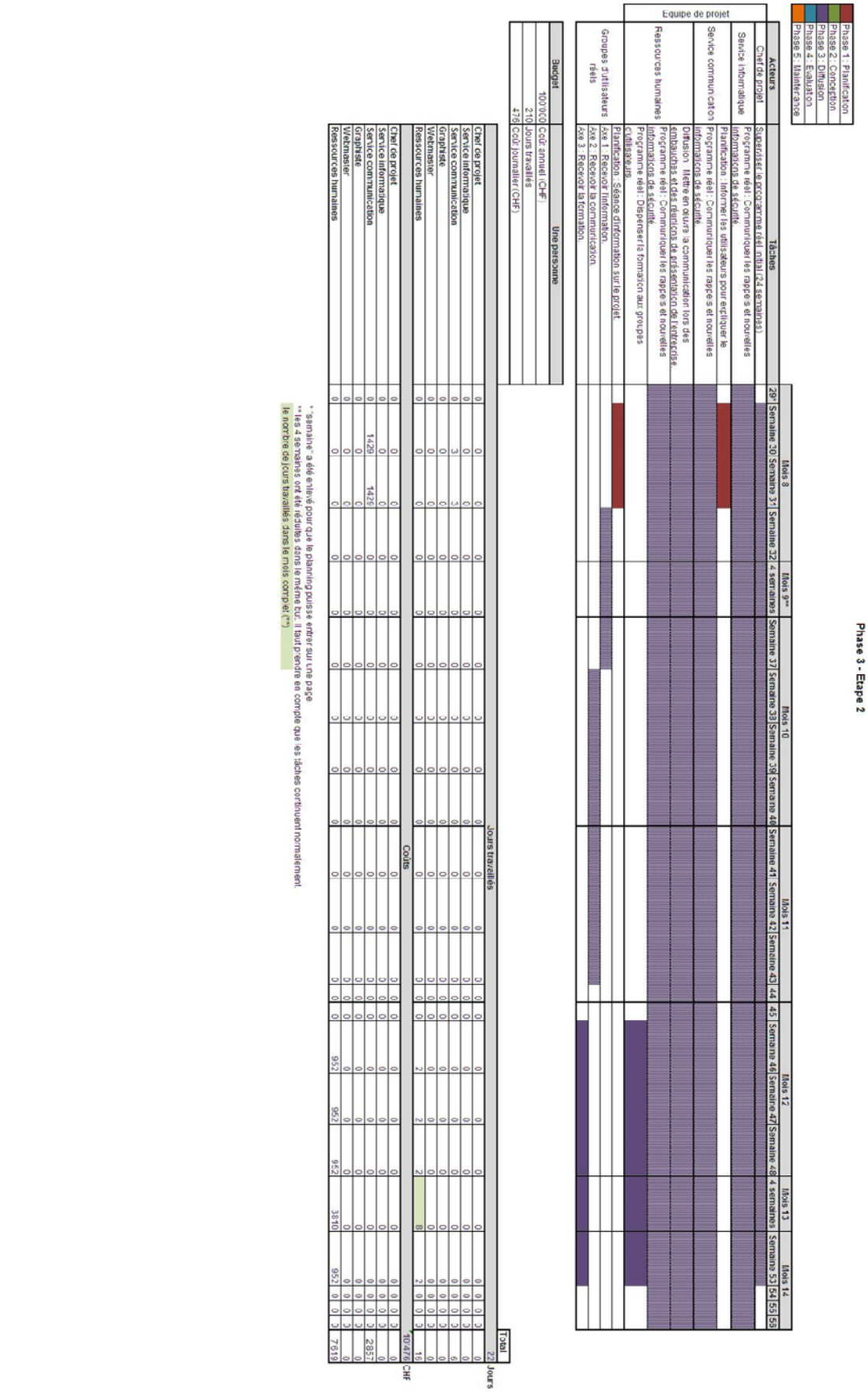
					Total	
	Jours travaillés				25	Jours
Chef de projet	5	5	5	0	15	
Service informatique	0	0	2	0	2	
Service communication	0	0	2	0	2	
Graphiste	0	0	2	0	2	
Webmaster	0	0	2	0	2	
Ressources humaines	0	0	2	0	2	
	Coûts				11'905	CHF
Chef de projet	2381	2381	2381	0	7'143	
Service informatique	0	0	952	0	952	
Service communication	0	0	952	0	952	
Graphiste	0	0	952	0	952	
Webmaster	0	0	952	0	952	
Ressources humaines	0	0	952	0	952	

Annexe 7 : Plan – Phase 2 – Conception

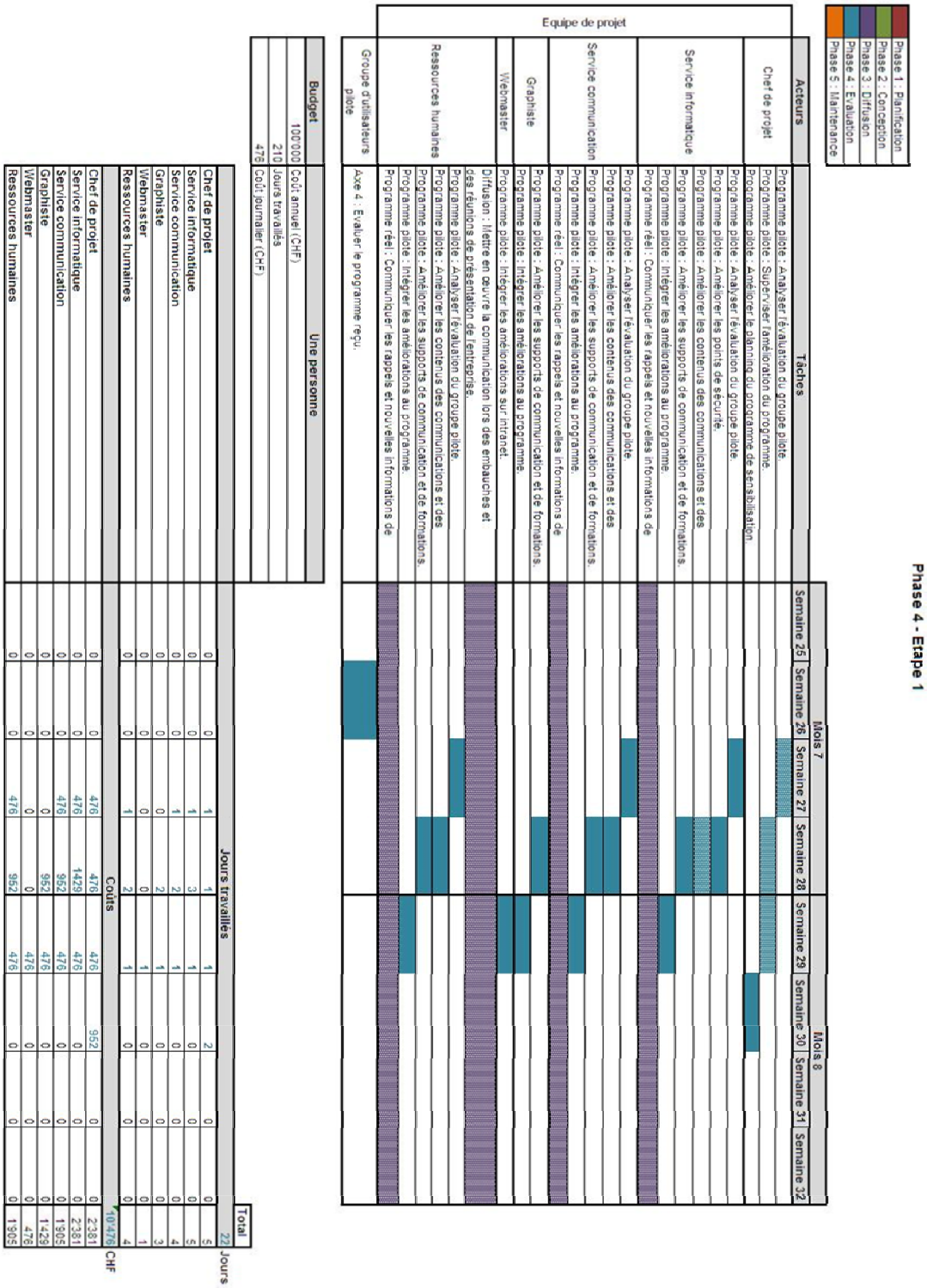


Annexe 8 : Plan – Phase 3 – Diffusion – Etape 1

Annexe 9 : Plan – Phase 3 – Diffusion – Etape 2



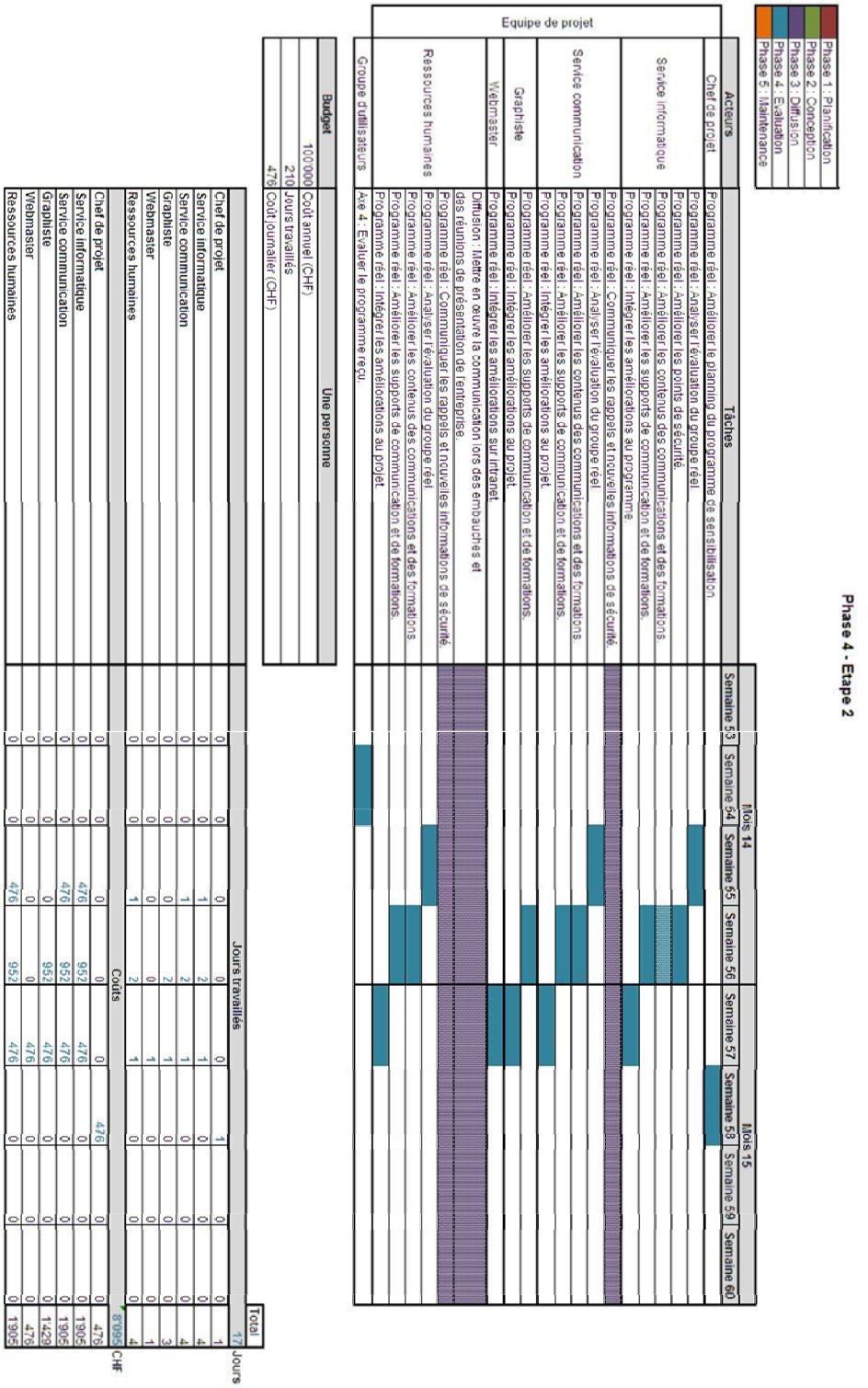
Annexe 10 : Plan – Phase 4 – Evaluation – Etape 1



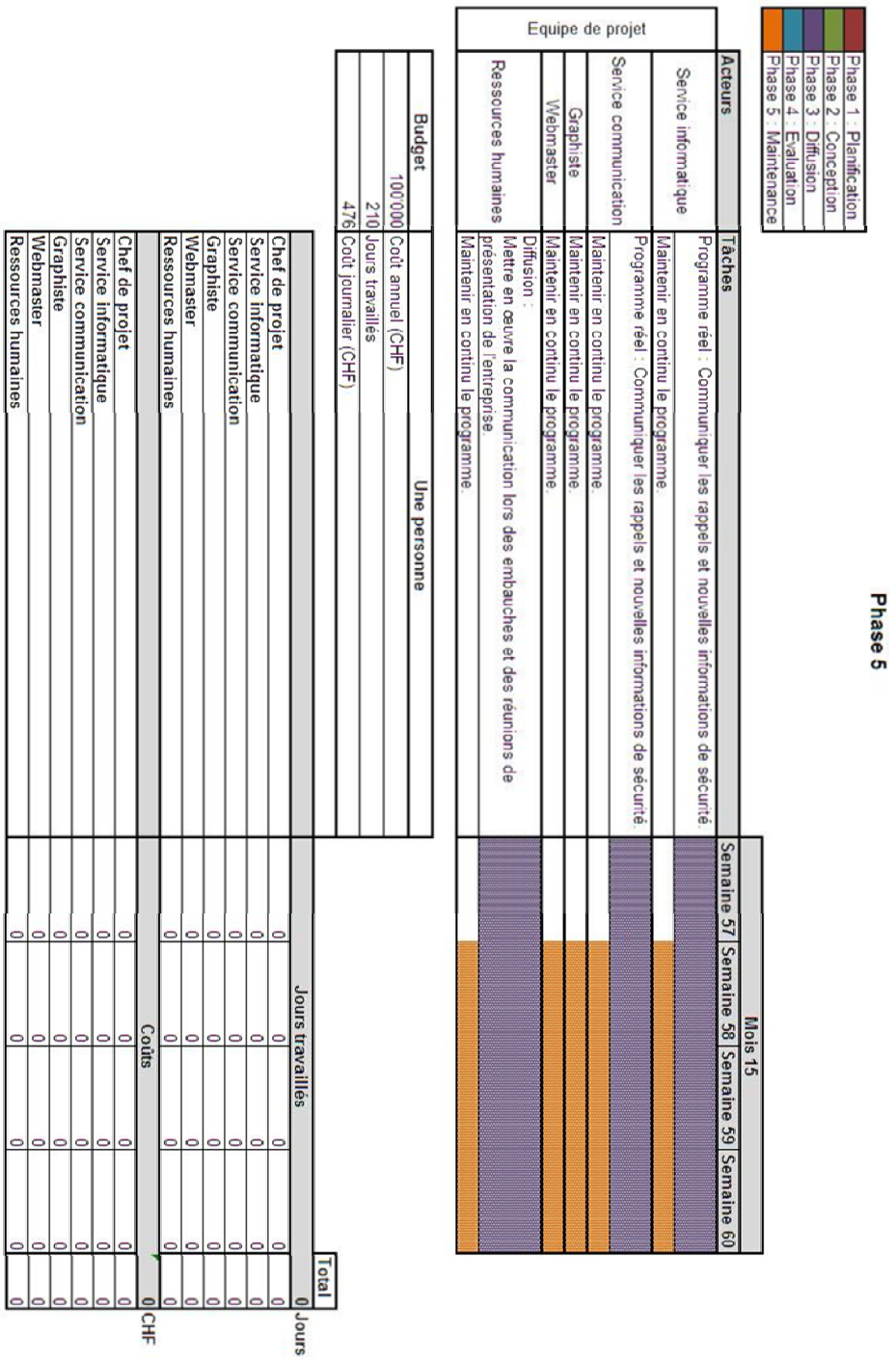
Budget	Une personne
Coût annuel (CHF)	100 000
Jours travaillés	210
Coût journalier (CHF)	476

	Jours travaillés								Total
Chef de projet	0	1	1	1	1	2	0	0	5
Service informatique	0	1	3	1	1	0	0	0	5
Service communication	0	1	2	1	1	0	0	0	4
Graphiste	0	0	2	1	1	0	0	0	3
Webmaster	0	0	0	1	1	0	0	0	1
Ressources humaines	0	1	2	1	1	0	0	0	4
	Coûts								10 476 CHF
Chef de projet	0	476	476	476	476	952	0	0	2381
Service informatique	0	476	1429	476	476	0	0	0	2381
Service communication	0	476	952	476	476	0	0	0	1905
Graphiste	0	0	952	476	476	0	0	0	1429
Webmaster	0	0	0	0	476	0	0	0	476
Ressources humaines	0	476	952	476	476	0	0	0	1905

Annexe 11 : Plan – Phase 4 – Evaluation – Etape 2



Annexe 12 : Plan – Phase 5 – Maintenance



Annexe 13 : Canaux de communication non adaptés

Canaux de transmission	Non faisable	Budget	Pourquoi
E-learning	x	Coûteux.	Il faut compter le temps pour le concevoir et établir le contenu. Ensuite, il y plus qu'à mettre en ligne ce qui existe déjà et le programme personnalisé au fur et à mesure de son utilisation par un collaborateur.
Réseau social d'entreprise	x	Peu coûteux.	Le réseau social de l'école se trouvant sur Facebook, est plus un moyen de communication externe qu'un moyen de communication interne. Donc les informations concernant la sécurité des informations de l'école n'est pas compatible avec ce canal de diffusion.
SMS professionnel	x	Coûteux.	Ce moyen de diffusion n'est pas adapté à la taille et à l'atmosphère de l'école, les employés n'ont pas besoin d'être au courant dans l'immédiat s'il y a un soucis de sécurité. Il serait considéré comme intrusif.
Brochure	x	Coûteux.	Il faut compter le temps à la concevoir, le coût du support et l'impression.
Objet quotidien	x	Coûteux.	Il faut compter le temps à concevoir les messages, le coût du support et l'impression.
Bande dessinée	x	Coûteux.	Il faut compter le temps à la concevoir, le coût du support et l'impression. Si par contre, elle est diffusé par ordinateur, le coût baisse.
Vidéo	x	Trop cher.	Les vidéos prennent malheureusement trop de temps de travail pour quelques minutes de sensibilisation. Il faudrait trouver les acteurs, du temps et mettre en place des scénarions.
Coaching	x	Trop cher.	Le helpdesk peut faire le même travail différement.
Formation externe	x	Trop cher.	Il n'y pas besoin de délocalisé une formation à la sensibilisation pour une structure comme l'école. Elle peut être faite par une équipe interne.
Jeux	x	Trop cher.	Il faudrait mettre en place tout un programme, trouver les collaborateurs pour établir celui et le temps. De plus, si un jeu est conçu sur ordinateur, il faudrait mettre les moyens pour avoir un jeu qui en vaille la peine.

Annexe 14 : Affiches de sensibilisation


COMME VOTRE DOMICILE,
VERROUILLEZ TOUJOURS
VOTRE POSTE DE TRAVAIL
Pensez à protéger
votre crédibilité
et la confidentialité de vos données.
Ne quittez pas votre ordinateur
sans en verrouiller l'accès.
WWW.CASES.LU
La sécurité de la technologie de l'information dépend de vous.
Soyez prudents et veillez consciencieusement sur votre matériel informatique. Verrouillez votre poste en cas d'absence, évitez les mots de passe trop simples, ne les partagez jamais et changez-les régulièrement, déclarez immédiatement toute anomalie à votre administrateur système et informez-vous régulièrement sur les risques informatiques sur cases.lu.
CASES
LUXEMBOURG
CYBERWORLD AWARENESS AND SECURITY ENHANCEMENT STRUCTURE