MASTER MANAGEMENT DES SYSTEMES D'INFORMATION - SPECIALITE PROFESSIONNELLE : EXECUTIVE MANAGEMENT DES SYSTEMES D'INFORMATION ET DE CONNAISSANCE

Promotion JB 2017

MEMOIRE

L'HUMAIN, ACTEUR DE LA PROTECTION DE L'INFORMATION

Rédigé et soutenu par SYLVIE DUCHARNE

Directeur de mémoire MONSIEUR YVES CHAUMETTE

Date de la soutenance 12 DECEMBRE 2018

L'UNIVERSITE N'ENTEND DONNER AUCUNE APPROBATION NI IMPROBATION AUX OPINIONS EMISES DANS CE MEMOIRE : CES OPINIONS DOIVENT ETRE CONSIDEREES COMME PROPRES A LEUR AUTEUR.

REMERCIEMENTS

Cet exercice fut rude et enrichissant !

Il m'a également permis de découvrir l'art, difficile, d'écrire et de synthétiser (si j'ai essayé !) sur un sujet qui m'a passionné.

Cette expérience m'a donné l'occasion de rencontrer des personnes formidables, qui se sont prêtées au jeu des interviews, des sondages et des échanges sur le sujet de la protection de l'information.

Particulièrement Monsieur Önder KELES RSSI de la société Carmignac et Monsieur Fabrice NERACOULIS, Responsable de la sensibilisation de la SNCF.

Je remercie également mes professeurs de l'Université Paris I Panthéon-Sorbonne, en particulier la directrice du Master Executive Management des Systèmes d'Information et de la Connaissance, Madame Selmin NURCAN.

Je ne remercierai jamais assez Monsieur Yves Chaumette, mon Directeur de mémoire, qui m'a guidé avec patience, et éclaira mes découvertes par son expérience et ses connaissances.

Et je n'oublie pas mes amis, qui m'ont soutenue tout au long du travail de ce mémoire et pendant le master et les belles rencontres durant la promotion 2017 : Aurélie, Caroline, David, Katlyne, Laetitia, Sarah, Sébastien,…

Je souhaite enfin exprimer ma gratitude à mon mari qui éclaire ma vie de son amour pour l'éternité.

INTRODUCTION

J'ai occupé plusieurs postes dans un cabinet d'avocats internationaux, Clifford Chance Europe LLP, à Paris entre 1997 et 2011. Mes missions étaient tournées vers la gestion de projets européens, la gestion du service formation et le maintien en condition opérationnel des applications du bureau de Paris. La notion de confidentialité et de protection de l'information est forte dans le milieu juridique. Malgré tout, aucune action de sensibilisation n'était mise en œuvre auprès des juristes ou des métiers supports.

J'évolue dans le domaine hospitalier en tant que Directeur des Systèmes d'information depuis 2011. J'ai également été Responsable de la sécurité des systèmes d'information d'un groupe hospitalier, suite au regroupement de plusieurs établissements de 2016 à mi 2018 et je suis redevenue DSI à partir d'avril 2018, d'un établissement de santé privé.

Les acteurs du milieu de la santé sont sensibles aux données des patients, mais ne sont pas sensibilisés à la protection de l'information et à la conséquence de certains de leurs actes (exemple : emploi de messagerie non sécurisée de type Gmail de Google pour échanger entre professionnels de santé).

Des mesures de contraintes techniques sont mises en place dans ces deux milieux. Les acteurs subissent cette protection sans vraiment comprendre pourquoi. Parfois les contraintes sont tellement élevées que le travail au quotidien peut en être affecté (ralentissement, multi-identification…). Ce point favorise le Shadows IT[1] et, de fait, l'exposition possible des informations sur la place publique.

➔ *POURQUOI AI-JE CHOISI CETTE PROBLEMATIQUE ?*

Les acteurs des organisations sont, pour la plupart, ignorants de la conséquence de leurs actes et de bonne volonté pour appliquer de bonnes pratiques afin de protéger leur organisation. Ils souhaitent aussi avoir moins de contrainte au quotidien avec leur outil informatique. Ce sont des êtres humains responsables et ils souhaitent être traités comme tel. Je n'aborderai pas, dans ce document, les cas de vol et d'espionnage intentionnel.

J'ai profité de mon expérience dans ces milieux différents, pour analyser ce que j'ai constaté sur le terrain, auprès des acteurs de l'organisation.

J'ai essayé de mixer des méthodes :

- De conduite de changement, appliquée dans la gestion de projet (ADKAR),
- D'enseignement aux adultes (Andragogie),
- De méthodes de terrain emprunté à l'industrie ou au marketing (Genba walk, Design Thinking),

afin de responsabiliser et transmettre les bonnes pratiques aux acteurs des organisations de manière éclairée et ludique.

Je n'ai, malheureusement, pas pu expérimenter toutes les méthodes sur le terrain, suite à des changements de vie professionnelle durant ce master et la rédaction de ce document.

---

[1] Shadow IT est un terme fréquemment utilisé pour désigner des systèmes d'information et de communication réalisés et mis en œuvre au sein d'organisations sans approbation de la direction des systèmes d'information. Source Wikipédia

➔ *DE QUELLE INFORMATION PARLONS-NOUS ?*

Une organisation protégera son patrimoine constitué de biens matériels mobiliers, immobiliers, ses stocks, ses outils, ses équipements… et de biens ou capitaux immatériels qui regroupent l'ensemble des informations et connaissances qu'elle détient.

Ce capital est représenté par :

- Les informations formelles : support papier, filmographique, ou numérique (exemple : les fonds documentaires, la presse, la télévision, la radio, les brevets, etc.)
- Les informations informelles : savoir-faire des personnels d'une organisation,
- Les droits incorporels : mémos de recherche, le dépôt des marques et brevets, les dessins et modèles et les droits d'auteur,
- Le patrimoine immatériel relatif à la relation client : réseaux relationnels et commerciaux, méthodes de distribution, marketing, engagements commerciaux, contrats,
- La recherche, l'innovation,
- L'histoire de l'entreprise elle-même.

Ces biens immatériels peuvent représenter jusqu'à 70 % de la valeur d'une organisation (secteur tertiaire) et sont visés par les concurrents ou certains états. Les uns et les autres peuvent employer des méthodes offensives et peu orthodoxes pour s'en emparer[2].

Les Japonais considèrent l'information comme un bien essentiel de l'organisation, cette notion est intégrée dans la constitution japonaise de 1868 qui indique la nécessité du Japon à « *chercher la connaissance dans le monde afin de renforcer les fondements du pouvoir impérial* »[3].

La protection des informations, donc de son savoir-faire, est indispensable pour assurer sa survie et sa continuité. Cela est possible uniquement si la sensibilisation à la protection de l'information est une priorité de l'organisation. Les informations sont considérées comme le « nouvel or noir[4] » de notre époque, donc elles sont convoitées par les voleurs, qui sont passés du braquage de banque à internet.

La réglementation européenne (RGPD), entre autres, va pousser l'organisation à mettre en place un programme de gouvernance fort, pour la protection de son patrimoine immatériel.

Cette ouverture vers le « cybermonde » induit de nouveaux risques de piratage, de dérives (parfois étatiques) pouvant aller jusqu'à de « cyberguerres ».

C'est pourquoi, la cybersécurité est, ou devrait être, une des composantes de la stratégie du système d'information suite à la généralisation de l'informatique, de l'internet, de la mobilité et de la transformation digitale des organisations. Cette cybersécurité est vitale tant pour les organisations, les états, l'économie que pour les hommes victimes de ces pirates.

La sécurité technique a ses limites pour protéger
Un système d'information.
L'humain est le pivot du système d'information.

---

2 DSE (Club des Directeurs de Sécurité des Entreprises).
3 Source docplayer.fr
4 Source docplayer.fr

Cet acteur de l'organisation fait partie intégrante du système d'information. Il manipule des informations dans le cadre de son activité. Par son expérience, il est apte à relever des incohérences et des activités suspectes dans son environnement.

Si cet acteur, a les moyens intellectuels, c'est-à-dire s'il a été sensibilisé à la protection de l'information et aux dangers qu'il pourrait rencontrer, il pourra être considéré comme un rempart efficace contre la criminalité digitale.

« *En organisation, la cybersécurité comprend trois maillons : la direction, qui alloue les moyens financiers et humains, le service informatique, qui va gérer ces moyens et l'utilisateur final, dont le comportement est influencé par la stratégie de son employeur. Si un seul de ces trois maillons est faible, toute la chaîne le devient* », indique Benoît Grunemwald, expert en cybersécurité chez Eset, éditeur de solutions de sécurité.[5]

La sensibilisation à la protection de l'information est indispensable à tous, dans une période où les « *cyberattaques* » ciblent autant les organisations, les établissements du domaine public ou privé que, les particuliers en se déployant à la sphère personnelle.

Nous pouvons tous être victimes d'une escroquerie ou d'un détournement de nos données privées usurpation d'identité, d'adresse courriel, vol de données de sa carte bancaire…

L'être humain, en face de son ordinateur constitue un des éléments « *faibles* » qu'un attaquant essaiera d'exploiter pour entrer dans le réseau interne de l'organisation ou pour détourner les fonds d'une organisation dans le cadre d'une attaque au président, par exemple[6]. Il est la cible, qui l'ignore, et il est également l'élément qui met en danger le système d'information par des comportements inconscients, insouciants ou désinvoltes qui démultiplient les risques.

Paradoxalement, c'est ce même être humain, qui, s'il connaît et comprend les menaces, pourra détecter et éviter une attaque.

Cet être humain peut être considéré comme un point fort car il est le dernier rempart contre la cybercriminalité.

Pour cette raison, il est essentiel de sensibiliser et d'éveiller pleinement la conscience des acteurs aux menaces informatiques et à la protection de l'information.

Nous emploierons le terme de « *protection de l'information* » à la place de « *sécurité du système d'information* » car le mot sécurité est restrictif et déplaisant par l'image qu'il véhicule de contraintes.

Nous nommerons les « *utilisateurs* » par le terme « *acteurs* », car le but de la sensibilisation est d'engager et de responsabiliser les acteurs de l'organisation, quelle que soit leur position dans la hiérarchie, dans la protection de l'information.

---

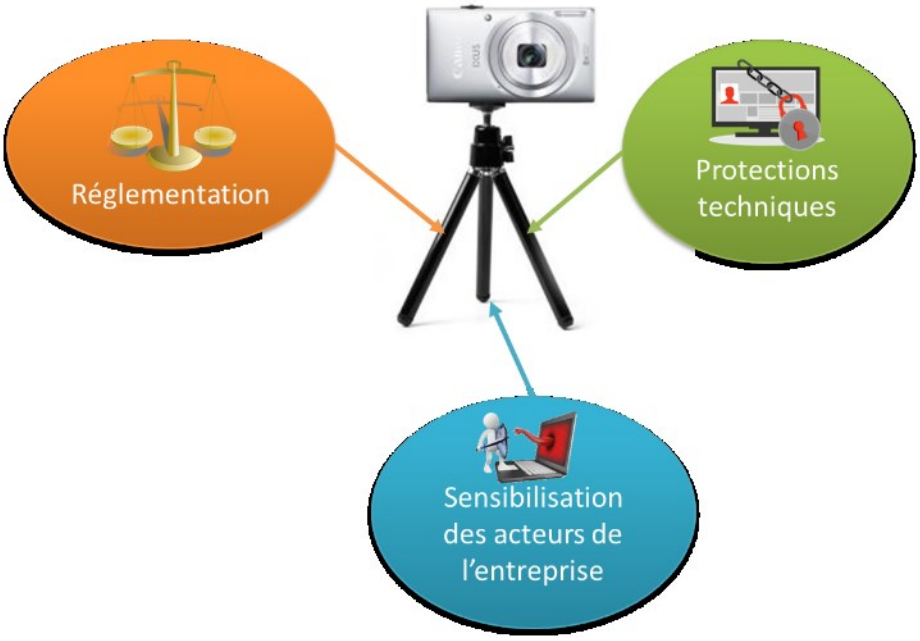
5 En savoir plus sur https://www.lesechos.fr/idees-debats/sciences-prospective/030599032649-lhumain-futur-rempart-contre-les-cyberattaques-2117161.php#4wU7qje7K4luYE37.99

6 L'escroquerie dite « au président » est une attaque de type ingénierie sociale (social engineering) qui va essayer de tromper un employé (généralement du service financier ou comptable) pour lui faire effectuer des virements impliquant d'importantes sommes (on parle de millions d'euros) vers des pays étrangers. Source (cyber-securite.fr, 2017)

Nous utiliserons le mot « organisation » pour désigner une organisation, une institution du domaine public ou privé, car la problématique s'adresse à l'ensemble du tissu économique à but lucratif ou non.

On peut comparer la protection de l'information à un appareil photo posé sur un trépied, qui serait composé de la réglementation, des moyens techniques de la protection et la sensibilisation des acteurs de l'organisation.

Si un des pieds est manquant, l'appareil photo tombe. Nous nous attacherons, dans ce mémoire à développer un de ces trois composants : la sensibilisation des acteurs de l'organisation.



ID n° 1 Trépied de la protection de l'information (symbole emprunté à M. Néracoulis, Responsable de la sensibilisation des personnels de la SNCF).

PROBLEMATIQUE

La problématique est :

L'humain, acteur de la protection de l'information

Qui peut être découpée en trois sous questions :

- Comment faire prendre conscience des dangers aux acteurs de l'organisation ?
- Comment sensibiliser les acteurs de l'organisation à la protection de l'information ?
- Comment faire pour qu'une connaissance devienne un réflexe ?

Le dictionnaire Larousse définit la sensibilisation comme « *Rendre quelqu'un, un groupe sensible, réceptif à quelque chose pour lequel il ne manifestait pas d'intérêt : par exemple : Les questions de sécurité sensibilisent vivement l'opinion.* »[7]

L'objectif d'une campagne de sensibilisation est de modifier le comportement d'individus, à obtenir l'appui des membres de l'organisation et plus largement à attirer l'attention du public. La sensibilisation du public est toujours un élément important, que l'on cherche à modifier les comportements individuels ou à induire des changements globaux. Le public pourra contribuer, par ricochet, à cette protection de l'information car il est sensible au devenir de ses propres données. [8]

L'approche auprès des acteurs de l'organisation, est-elle la bonne ? Les messages sont-ils exprimés de façon à toucher l'auditoire ?

La démarche de sensibilisation permet, en étant sur le terrain, de remonter des problèmes, inconnus jusqu'alors et déclencher une prise en compte de celui-ci par les acteurs concernés.

L'analyse de ces problèmes permet de lancer une réflexion sur sa résolution et d'agir à son éradication.

La sensibilisation est une étape du processus de la politique de sécurité du système d'information. Son but est de provoquer un changement des habitudes tant au niveau individuel que collectif.

L'objectif de cette démarche est de :

- Transformer l'homme en ami de la protection de l'information de l'organisation,
- Déclencher une prise de conscience et une action collective,
- Stimuler les personnes impactées par la protection de l'information,
- Encourager des idées novatrices afin de modifier un problème ou apporter une solution à un besoin,
- Modifier les réflexes individuels, les habitudes d'usage de l'outil informatique, l'utilisation d'internet dans l'organisation et toucher la sphère privée (utilisation de la carte bancaire sur internet, l'utilisation du WIFI public etc.),

---

7 Source dictionnaire Larousse

8 Selon les résultats de l'étude KPMG « Crossing the line - Staying on the right side of consumer privacy » - conduite entre avril et mai 2016 dans 24 pays, en partenariat avec le cabinet 3Gem - plus de la moitié des consommateurs dans le monde sont inquiets de l'utilisation qui peut être faite de leurs données personnelles ; les consommateurs français parmi les plus vigilants, et donc les plus exigeants en termes de transparence et de cybersécurité. Moins de 10 % des consommateurs estiment avoir le contrôle sur l'utilisation de leurs données personnelles https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2016/11/crossing-the-line.pdf

- Influencer le top management, afin de les rendre plus sensibles aux réalités de la complexité, de la situation de la protection de l'information et des moyens à engager.

Cet état de guerre aspire à provoquer l'engagement des personnes partageant un centre d'intérêt commun (la défense de l'organisation ou de leurs données personnelles) autour d'un projet visant à satisfaire le besoin de connaissance de cette criminalité et le besoin de l'organisation à protéger les informations qu'elle détient (données des patients, données financières, données stratégiques, etc.).

Les personnes concernées démontreront leur engagement vis-à-vis de leur organisation en étant elles-mêmes actrices du changement et de par leur volonté de contribuer à un projet de grande ampleur afin de faire face à des criminels tout en restant derrière leur écran !

La conduite du changement s'opérera durant tout le projet, car une campagne de sensibilisation s'échelonnera sur plusieurs semaines, voire plus longtemps et sera récurrente.

Le chemin sera long car la motivation est difficile à maintenir sur une longue période., nous serons amenés à associer des pratiques de gestion mobilisatrices et mettre en avant les efforts concédés par les acteurs du projet. Ces actions permettront l'éclosion de comportements et d'attitudes favorisant l'engagement.

La démarche qui sera menée devra être logique, visuelle et impactant. Toute exagération mettra en péril notre démarche car, les acteurs les plus dubitatifs mettront tout en œuvre pour anéantir sa crédibilité et la faire échouer.

La méthode d'analyse de risques sur un parcours, sera utilisée. C'est-à-dire identifier les dangers et les besoins des acteurs, internes et externes à l'organisation, par rapport à un parcours sur le terrain, qui s'apparente à un processus. Exemple : la visite d'une usine par un client, le parcours d'hospitalisation d'un patient, les mouvements de personnels dans une entreprise, etc. Cette approche s'inspire du Genba Walk (voir §3.3.4 page 100), cette méthode peut s'appliquer à tout type d'entreprise privée et / ou publique.

Celle-ci à l'avantage de nous projeter sur le terrain, la réalité, auprès des acteurs, comprendre leur problématique, commencer la sensibilisation en toute connaissance de cause et renvoyer des exemples concrets aux personnes concernées tirés de leur propre expérience.

Cela nous permet également de tisser une relation de confiance et d'induire un réflexe de retour vers le responsable de la protection de l'information en cas d'identification d'un danger ou de doute.

Les acteurs sont considérés comme des « *enfants ignorants »* et le garant de la protection de l'information comme le « *sachant* » menant les acteurs sur le chemin de la connaissance. Cela s'apparente à une relation parents/enfants : le parent transmet les connaissances pour que l'enfant devienne autonome et armé face à la vie.

La démarche peut être accompagnée de manières différentes, par exemple :

- Organiser une activité ciblée afin d'examiner si le besoin est avéré lors une session d'information,
- Profiter d'une thématique comme le « mois de la Cybersécurité » organisé chaque année par l'ANSSI,
- Utiliser une multitude d'activités et de supports comme la distribution de nouveaux calendriers pour la nouvelle année avec des messages de sécurité visibles,

- Faire appel à des commanditaires, qui sont friands de démontrer leur savoir-faire et viennent avec une valise entière de gadgets,

Le résultat de l'enquête menée auprès des responsables de la sécurité du système d'information de divers secteurs économiques, permet de dégager des tendances de supports de communication et méthodes de sensibilisation utilisées. L'analyse des commentaires apportés par les répondants laisse apparaître des pistes de réussite (voir page 2.4 page 63).

Parallèlement les interviews ciblées et le suivi d'un binôme « *cabinet de gestion de fonds et la société Wavestone* »[9], nous permettra de vérifier comment les campagnes de sensibilisation fonctionnent sur un secteur économique de la finance.

À côté, l'enquête, basée sur des scénarios d'incidents, menée auprès des acteurs nous donnera des indications sur les bornes que les acteurs sont prêts à franchir ou pas.

[9] Cabinet spécialisé en protection de l'information

CHAPITRE 1
RISQUES ET MENACES

"Mieux je connais, plus je réfléchis, mieux j'agis"
Gérard Malglaive[10]

[10] Gérard Malglaive a un parcours lié à la formation des adultes et à l'univers de la formation professionnelle et ses mutations Il a créé l'Institut national de formation des adultes (INFA).

1.1. INTRODUCTION

Le système d'information est confronté à diverses menaces internes et externes, à l'origine de comportements humains inadéquats en matière de sécurité.

Ces menaces sont de plus en plus présentes dans les organisations.

Ce chapitre présente les origines du danger, les prévisions en matière de cybercriminalité et que protéger.

1.2. ORIGINE DE LA CYBERCRIMINALITE

Les premiers cas de vol d'informations sont apparus avant l'invention d'internet et de sa démocratisation.

Le concept du malware est apparu en 1940. John Von Neuman[11], mathématicien et physicien, de son état, a travaillé sur des méthodes de « fabrication » dans le cadre des automates mathématiques à reproduction automatique.

Lionel Penrose[12], mathématicien britannique, en 1959, publie un article « *Self-reproducing Machines* » dans le Scientific American. Il parle d'un modèle élémentaire à deux dimensions qui peut être activé, se multiplier, muter et attaquer. À la suite de cette publication, Frederick G. Stathl écrit ce modèle en code machine sur un IBM 650. À ce moment-là il n'était pas question de fabriquer des malwares. Ces études ont été reprises dans le cadre de la robotique et de l'intelligence artificielle.

Des ingénieurs de la société « *Bell Telephone* » créèrent, en 1962, un jeu, nommé *Darwin*, qui consistait à détruire les programmes de concurrents en ayant la possibilité de se multiplier.

Les années 1970 ont vu le premier virus apparaître sur les réseaux dédiés (voir §1.1 page17) et les années 1980 les premières épidémies contaminer les ordinateurs. La transmission se faisait via des disquettes d'installation (exemple *Elk Cloner*), le processus identique sera utilisé avec les CdRom en 1994.

La première contagion de virus compatibles IBM est apparu en 1986, il ne nommait Brain, le virus se propagea à travers le monde en quelques mois. Ralf Burger, programmeur allemand, inventa, la même année un programme capable de se copier.

En 1987, le célèbre virus *Lehigh,* découvert par l'université de Pennsylvanie était le premier à endommager les données, Il lançait une règle qui supprimait toutes les données de valeur avant de s'autodétruire.

Ken Van Wyk [13] ouvra, le 22 avril 1988, le premier forum *Virus-L,* sur le réseau Usenet consacré à

---

[11] John von Neumann, né Neumann János Lajos en 1903 à Budapest et mort en 1957 à Washington, est un mathématicien et physicien américano-hongrois. Il a apporté d'importantes contributions tant en mécanique quantique qu'en analyse fonctionnelle, en théorie des ensembles, en informatique, en sciences économiques ainsi que dans beaucoup d'autres domaines des mathématiques et de la physique. Il a de plus participé aux programmes militaires américains.

[12] Psychiatre britannique, généticien médical, pédiatre, mathématicien et théoricien des échecs, qui a effectué un travail de pionnier sur la génétique du retard mental.

[13] http://virus.wikidot.com/

la sécurité contre les virus.

Le ver Morris, en 1988, infecta 600 systèmes informatiques aux états Unis, dont la NASA Ce ver exploitait une faille d'UNIX et a innové en collectant les mots de passe pour s'introduire dans les systèmes. Ce malware avait la particularité de se démultiplier et de saturer les réseaux. Celui-ci a engendré 96 millions de dollars de pertes.

Le premier antivirus est apparu en 1988, *Dr Solomon's Antivirus Toolkit*[14]. Cette société fut rachetée par Network Associates qui devint McAfee, Inc. Les sociétés virent le jour dès 1989, comme *V* de Kaspersky, F-Prot, ThunderBYTE, Norman Virus Control et Virscan for MS-DOS (créé par IBM)[15]. Norton Antivirus, Central Point Antivirus et Untouchable ont été créés en 1991.

Dès 1990, les virus devinrent Polymorphes (exemple de *Chameleon*). Le code de ces virus est crypté et se modifie à chaque cycle d'infection, ce qui les rend indétectable par les antivirus, basés sur des recherches contextuelles.

Les antivirus, ont, eux aussi évolué en utilisant des algorithmes capables d'identifier ces virus. La nouvelle entité EICAR (Centre européen de recherche contre les virus informatiques) voit le jour. Elle regroupe les éditeurs d'antivirus et est reconnue dans son domaine.

300 virus sont recensés en 1991. Le système d'exploitation est attaqué (MS Dos) et plus particulièrement l'IBM PC, ainsi que Windows virus : *Win. Vir_1_4*. Les états prennent, enfin conscience du phénomène et créés des brigades de lutte contre la cybercriminalité comme à Scotland Yard.

Les logiciels sont aussi concernés, avec le Pack office (MS Word notamment) en 1995. Les sociétés d'antivirus doivent redévelopper leur produit afin de détecter ce genre de contamination. Les autres systèmes ne sont pas en reste, comme LINUX, lui aussi touché en février 1997 (*Linux Bliss*) et, l'imagination des attaquants suit les usages : le courriel est utilisé comme vecteur de propagation (MS Mail) ainsi que l'ancêtre des messageries instantanées mIRC (Internet Relay Chat).

Melissa, est le premier ver, combinant l'usage de MS Word et internet pour faire des ravages. Le virus balaie le carnet d'adresses de MS Outlook et envoie une copie de lui-même par messagerie ; l'épidémie a été mondiale et a causé des dizaines de millions de dollars de dégâts. Une autre faille a été exploitée via la messagerie et internet explorer. Le virus se propageait par courrier électronique et contaminait son hôte dès lecture de celui-ci (Bubbleboy et KaKWorm) (voir les dates marquantes en Annexe n°10 page 185).

1.3. DANS QUEL CYBERMONDE VIVONS-NOUS ?

Les premières déferlantes de cybercriminalité sont apparues dans les années 1980 avec la démocratisation de l'usage des messageries électroniques. Les boîtes aux lettres ont été la cible préférée des virus ou logiciels malveillants (exemple : l'escroquerie « *A la Nigériane* »[16]). La deuxième vague a eu lieu dans les années 1990, avec la mise en avant des navigateurs Web. Ceux-

[14] Développé par Alan Solomon, un programmeur anglais Source Wikipédia

[15] Source Wikipédia

[16] Fraude 419 (aussi appelée scam 419, ou arnaque nigériane) est une escroquerie répandue sur Internet. La dénomination 4-1-9 vient du numéro de l'article du code nigérian sanctionnant ce type de fraude. Cette escroquerie abuse de la crédulité des victimes en utilisant les messageries électroniques (courriels principalement) pour leur soutirer de l'argent.

ci transportaient des virus, via la connexion internet ou des sites infectés jusqu'à notre ordinateur.

La numérisation des informations a permis de faire progresser le stockage et l'échange d'information entre les organisations, les états et les êtres humains. À côté de cette organisation 3 milliards de malwares attaquent les ordinateurs chaque année depuis les années 2000.

Le Big data, avec la collecte d'informations des réseaux sociaux (voir Annexe n°9 page 185), au début des années 2000 a déclenché un déferlement sans fin des cybercriminels. Ils ont pillé les données personnelles pour en tirer des bénéfices comme le vol d'identité, la création de carte bancaire, le montage de fraudes financières. Le vol est effectué directement ou indirectement[17]. Le « business » de ces gangs mafieux internationaux, leur rapporte environ un demi-milliard de dollars par an. La cybercriminalité est un métier (malhonnête) à part entière.

Attaques par « *ransomware* » (voir §1.6.1 page 42 et les attaques connues Annexe n°10 page 185), infections d'ordiphone, cyber-espionnage étatique, objets connectés… (voir Annexe n°8 page 183) ; la cybercriminalité est réelle et provoque des craintes.

Les cybercriminels suivent les progrès, les usages et veulent atteindre ces données pour des raisons financières.

Des professionnels ou particuliers s'adonnent à l'extorsion d'argent auprès d'utilisateurs avec des rogues (rançongiciels ou riskwares[18] – voir 1.6.1 page 42 et Annexe n°12 page 187). Ils créent également des réseaux de botnet[19] pour envoyer, massivement des pourriels et sont rémunérés sur le nombre adressé. Les criminels pratiquement également les attaquent DDoS[20] auprès de boutiques en lignes, de sites bancaires ou de jeux en ligne.

Certains développent des publiciels (*adware)*, programmes qui redirigent les internautes vers des sites payants ou infectés.

Des chevaux de Troie sont positionnés sur les ordinateurs afin d'espionner leur utilisateur et leur dérober de l'argent sur leur compte bancaire. Malheureusement, les chevaux de Troie, font d'autres victimes que les organisations ou les particuliers : le crash de l'avion 5022 de la Spanair en août 2008 pourrait être dû à un cheval de Troie, qui aurait déréglé le système d'alerte en l'empêchant de fonctionner.[21]

L'année 2017 a connu ses lots d'attaques avec *WannaCry* (voir Annexe n°13 page 188) et ses variables ; les cybers attaquants perfectionnent leurs outils et créés de nouveau type de malware comme *Locky*. (Voir §1.6.2 page 45).

Certains malwares fonctionnent en duo comme *Cerber* et le virus *Kovter*. Le premier détourne

---

17 Comme en 1997, les premiers chevaux de Troie étaient utilisés pour voler les mots de passe d'AOL pour accéder gratuitement à internet. Le même principe est appliqué, aujourd'hui aux logiciels, pour lesquels les pirates cherchent et dérobent les clefs de licences, pour utiliser les applications gratuitement.

18 Le ransomware consiste à s'infiltrer sur un système d'information (généralement au travers de courriels frauduleux), puis à en chiffrer tous les fichiers, et enfin, à exiger une rançon à payer en bitcoins.

19 Réseaux de robots ordinateurs (botnets) ou zombies. Des ordinateurs de particuliers peuvent être utilisés, comme relais, sans qu'ils le sachent à des fins criminelles.

20 Saturation de la bande passante

21 Source fr.wikipedia.org

l'attention des équipes techniques afin que le cheval de Troie (voir §1.6.1 page 42) s'installe et joue son rôle en toute quiétude.

Les personnes malveillantes sont à la pointe du progrès et arrivent à contourner des systèmes d'identification 3d (emprunte digitales[22] ou contrôle de l'iris[23]) au moyen d'une simple impression papier et quelques astuces.

Selon « *Le panorama des menaces informatiques en 2017* »[24] de Verizon, ceux-ci indiquent que 90 % des attaques envers les organisations sont attribuées à des groupes reliés à des états ; les PME innovantes sont la cible majeure du pillage intellectuel. La négligence des organisations, à sécuriser correctement leur réseau WIFI, permet aux cybers attaquants de s'introduire dans leur réseau et de relever des courriels, des documents stratégiques et des données personnelles.

➔ *NOUVEAUX USAGES, NOUVEAUX OUTILS ET NOUVELLES ATTAQUES*

Dès l'an 2000, le téléphone mobile a été touché par *Timofonica* virus [25] de téléphones mobiles impactant les réseaux téléphoniques Movistar de Telefonica. Palm Pilot[26] a été touché par le premier cheval de trois *liberty* en août.

L'emploi des messageries instantanées se développe (comme ICQ, IRC, MSN Messenger) ainsi que les réseaux de partage de fichiers (peer to peer). Donc les pirates continuent de s'adapter et utilisent ces nouveaux supports pour contaminer les ordinateurs.

Les bases de données sont aussi touchées comme My SQL, base de données, largement utilisée pour la création de sites internet interactifs. En 2003, les vers *Lovesan* et *Slammer* ont infecté plusieurs centaines de milliers d'ordinateurs, à travers le monde en quelques minutes. Les proxys sont aussi touchés[27].

Toutes les failles exploitables sont exploitées.

Réseau électrique : Le réseau électrique de la ville de Kiev a été piraté en décembre 2016. Un cinquième de la ville est resté dans le noir, faute d'électricité, car celle-ci était coupée. *ESET* et *Drago INC*[28] ont découvert que le réseau avait été manipulé par des pirates informatiques. C'est la deuxième fois que la ville de Kiev est attaquée.

Smart city : IBM a testé les vulnérabilités de villes intelligentes aux USA (qui utilisent la collecte

---

22 Une organisation experte dans le domaine a réussi à hacker le lecteur d'empreinte de l'iPhone extrêmement simplement, avec de la pâte à modeler. Deux chercheurs travaillant pour la Michigan State University ont mis au point une technique permettant de pirater la plupart des smartphones à lecteurs d'empreintes en à peine 15 minutes. http://www.phonandroid.com/15-minutes-peuvent-hacker-importe-quel-lecteur-empreinte.html

23 Un groupe de hackers européens du nom de Chaos Computer Club (CCC) est parvenus à duper le dispositif du smartphone Galaxy S8 à l'aide d'une simple photo d'œil. Photographiée puis imprimée, le cliché de l'iris a ensuite été recouvert par une lentille de contact de façon que le portable l'identifie à l'aide de la reconnaissance faciale. http://www.phonandroid.com/samsung-galaxy-s8-scanner-iris-peut-etre-trompe-par-simple-photo-oeil.html

24 http://www.silicon.fr/hub/malwarebytes-hub/le-panorama-des-menaces-informatiques-en-2017?inf_by=59b24379671db8da448b480a

25 Source Wikipédia

26 PDA (Personal Digital Assistant)

27 Source www.senat.fr

28 ESET est un fabricant de logiciels antivirus slovaque. Dragos Inc est une entreprise américaine de sécurité spécialisée dans les infrastructures critiques.

de données électroniques pour gérer les ressources de la ville), dans l'optique de se mettre à la place de criminel et de mener une attaque de grande ampleur à distance. Les chercheurs *d'IBM Threatcare* et *X-Force Red*[29] ont découvert 17 failles de sécurité dans quatre villes, dont 8 critiques. Les résultats révèlent des failles de sécurité courantes comme : les mots de passe par défaut non modifiés, le contournement d'authentification et l'injections de code SQL.

Les satellites : tous les ans à lieu le *Black Hat USA*[30]. Cette année 2018, Ruben Santamarta, consultant en sécurité chez *IOActive* [31] a révélé que le système de communication par satellite SATCOM a des failles de sécurité. Ce satellite est utilisé par les bateaux, les avions et les militaires du monde entier.

Les assistants vocaux : Siri d'Apple, Google Home, Alexa de Amazon, Cortana de Windows facilitent la vie des personnes. Ils leur permettent de faire des recherches sur internet ou sur leur ordinateur, d'écrire à leur place, de commander sur internet, d'interagir avec leur domicile (smart home, domotique) ou leur voiture (smart car) etc.

Des failles sont apparues et ont démontré que ces outils ne se contentaient pas de vous rendre service mais aussi de vous espionner. Ces assistants seraient attaquables par l'intermédiaire d'ultrasons. Les pirates informatiques pourraient manipuler vos assistants en introduisant des commandes inaudibles pour des êtres humains, dans des vidéos ou de la musique afin d'envoyer de l'argent ou des messages à l'insu de son propriétaire.

Geoffrey Delcroix[32], les considère comme des « *espions à domicile* ». George Orwell faisait référence à un outil d'espionnage permanent dans son roman 1984 !

Conceptuellement, ces machines n'ont pas de bouton marche/arrêt, donc elles sont toujours en marche, prête à réagir à votre appel. Le but inavoué des grandes marques, comme Amazon, Google and Co, est de collecter des données personnelles et de les exploiter à des fins économiques.

Donc, nous devons débrancher ces machines lorsque nous n'en avons pas besoin, ou accepter que notre vie privée et nos données personnelles soient exploitées à des fins mercantiles.

Vulnérabilité des ordinateurs : nous devrions déjà nous passer de nos ordinateurs transformables en espion. Les écouteurs et les haut-parleurs sont équipés de microphone. Donc tout écouteur branché à un ordinateur peut être transformé en espion. Certaines puces audio peuvent modifier la fonction d'un port audio dans le logiciel même ; ce point est connu de tous les techniciens, c'est une spécificité de la carte mère d'un ordinateur !

Les cybercriminels peuvent espionner vos conversations et les stocker sur des serveurs par

---

29 IBM X-Force Red est un groupe de professionnels de la sécurité et de hackers éthiques dont l'objectif est d'aider les entreprises à identifier les vulnérabilités au sein de leurs réseaux informatiques, de leurs matériels et leurs applications logicielles avant les cybercriminels.

30 Les Conférences Black Hat (ou Black Hat Briefings) sont un événement qui rassemble officiellement des experts des agences gouvernementales américaines et des industries, américaines ou non, avec les hackers les plus respectés de l'« underground ». Ces forums sont régulièrement organisés à Las Vegas (Black Hat USA), Amsterdam (Black Hat Europe), Tokyo (Black Hat Japan), et Singapour (Black Hat Asia). Un événement est spécialement organisé pour les agences fédérales américaines à Washington (Black Hat Federal), et un autre sur la sécurité sur les systèmes d'exploitation Microsoft Windows (Black Hat Windows Security).

31 Société de recherche en sécurité située à Seattle

32 Membre du laboratoire d'innovation de la Commission nationale de l'informatique et des libertés (CNIL),

l'intermédiaire d'internet et ils peuvent également, écouter vos discussions via vos écouteurs, à des kilomètres de distance avec une qualité de son acceptable, vu que nous portons généralement les écouteurs autour du cou ou posés près de nous.

Devons-nous nous passer des évolutions technologiques pour autant ? La réponse est non ! Nous devons être informés des dangers et des possibilités de détournement des informations et des données personnelles.

Le cloud est à prendre en compte au vu de l'évolution du choix des organisations dans leurs investissements et le fameux « virage numérique » :

- 70 % des entreprises investissent dans le cloud[33]
- 73,6 milliards de dollars[34] dans le SaaS (Software-as-a-Service)[35]
- 40,8 milliards de dollars sur le IaaS (Infrastructure-as-a-Service)[36]. Ce secteur subit la croissance la plus forte avec une augmentation de 35,9 % par rapport à 2017 [37].
- 69 % des entreprises sont en multi cloud, elles utilisent deux ou plusieurs clouds avec au moins deux fournisseurs[38].

Faut-il avoir peur du Cloud, du Big data et du machine learning [39]?

Certains pensent que ces nouvelles offres technologiques, pourront confondre les cyber terrorisme, car la faculté de calculs et la prédiction d'attaques seront possibles à travers la puissance de calcul mis à disposition dans les Datacenter (§1.5.1 page 29).

Nous n'avons pas été confrontés à ces choix technologiques au travers de nos expériences ou relations professionnelles ; nous ne pourrons pas répondre sur la légitimité de ces choix vis-à-vis de la protection de l'information. Il paraîtrait logique que le machine learning et, l'intelligence artificielle aideront les humains en charge de ces clouds pour détecter des compromissions d'informations. La puissance du machine learning est supérieure, en délais d'analyse de l'information, au cerveau humain.

1.3.1. APRES LES ATTAQUES LOGIQUES, LES ATTAQUES PHYSIQUES

Janvier 2018, Intel révélait une faille de sécurité sur ses microprocesseurs, existante depuis 1995 ! Deux vulnérabilités nommées « *Meltdown et Spectre* » affectent les puces Intel. C'est officiellement la première attaque sur des composants matériels.

Ces dysfonctionnements de sécurité permettent l'accès à des zones de mémoires utilisées par des

---

33 Etude KPMG 2018
34 Etude Gartner 2018.
35 SAAS veut dire « Le logiciel en tant que service » ou software as a service est un modèle d'exploitation commerciale des logiciels dans lequel ceux-ci sont installés sur des serveurs distants plutôt que sur la machine de l'utilisateur. Les clients ne paient pas de licence d'utilisation pour une version, mais utilisent librement le service en ligne ou, plus généralement, payent un abonnement.
36 IAAS veut dire : « infrastructure en tant que service ». C'est un modèle d'organisation où l'entreprise dispose sur abonnement payant d'une infrastructure informatique (serveurs, stockage, sauvegarde, réseau) qui se trouve physiquement chez le fournisseur.
37 Etude Gartner 2018
38 Etude 451 Research 2018
39 Apprentissage automatique

logiciels en cours de fonctionnement. Cet état permettrait à un malware de lire des informations stockées dans les logiciels dont des mots de passe. Plusieurs applications sont vulnérables dont Windows.[40].

Fin janvier 2018, Cisco [41]révélait une grave faille sur la plupart de ses équipements de sécurité réseau. Le bug CVE-2018-010 est côté au niveau de sévérité maximale de 10.[42]

1.3.2. LA SANTE CIBLE DES ATTAQUES

Sergey Lozhkin, expert en sécurité chez Kaspersky Lab., a démontré comment il est facile pour les pirates informatiques de compromettre les dispositifs médicaux (voir Annexe n°7 page 182) et par conséquent les infrastructures de soins de santé. [43]

La société *TrapX*[44], a révélé que des cybercriminels ont été pris en flagrant délit en train de reconditionner et dissimuler des outils avancés dans du matériel plus ancien. Certaines versions de Windows sont actuellement ignorées par les logiciels de sécurité, étant jugés dépassées.

La société *TrapX Security*, toujours, a réalisé une étude sur les cyberattaques dirigées et détectées par les établissements de santé entre fin 2015 et début 2016[45] : les attaques contre les dispositifs médicaux augmentent, car ceux-ci comportent des « portes dérobées » ou des possibilités d'accès à distance non sécurisés. Les pirates informatiques s'introduisent dans les appareils, espionnent, volent les données et déploient des logiciels malveillants sur le réseau de l'organisation. Des failles de sécurité ont été révélées en 2017 sur des appareils médicaux, tels que les stimulateurs cardiaques [46] ou les pompes à insuline[47]. (Voir Annexe n°6 page 182).

La société *MyHeritage DNA* propose des tests ADN dans le cadre de recherches généalogiques. Celle-ci a été piratée en octobre 2017, l'information a été révélée en juillet 2018 ; les courriels et mots de passe de 92 millions d'utilisateurs ont été retrouvés sur un serveur privé. Depuis quelques années, une multitude de laboratoires voient le jour et fournissent tout ce que nous souhaitons savoir sur notre génome ou celui de nos proches. Quid des informations très personnelles qui pourraient être révélées sur des personnages publics ?

- Nous avons relevé quelques événements survenus les premiers mois de l'année 2016 dans plusieurs centres hospitaliers :
  - Ransomware attaquant plusieurs hôpitaux en bloquant l'accès du personnel aux systèmes essentiels et impossibles à supprimer pendant des semaines[48],

---

40 Source : https://secureidees.com/?s=Meltdown

41 Cisco Systems est une entreprise informatique américaine spécialisée, dans le matériel réseau (routeurs et commutateurs Ethernet), et les serveurs depuis 2009.

42 La faille majeure annoncée par Cisco qui affecte la fonctionnalité WebVPN d'une série d'appliances : Firepower 2100 Series, Firepower 4110, Firepower ISA (Industrial Security Appliance) 3000 Series, ASA (Adaptive Security Appliance) 5500 Series, ASA 5000-X (pare-feu de nouvelle génération), ASA 1000V (Cloud Firewall) mais aussi l'appliance virtuelle ASAv, ainsi que son logiciel FTD 6.2.2 (Firepower Threat Defense). Si l'alerte est si inquiétante, c'est que le bug découvert (CVE-2018-010) est affublé d'une sévérité maximale de niveau 10.

43 http://securityaffairs.co/wordpress/44558/cyber-crime/hack-medical-devices.html

44 Société spécialisée dans la détection d'attaque en temps réel. https://trapx.com/

45 https://securityledger.com/wp-content/uploads/2015/06/AOA_MEDJACK_LAYOUT_6-0_6-3-2015-1.pdf

46 https://threatpost.com/fda-recalls-465k-pacemakers-tied-to-medsec-research/127750/

47 http://thehackernews.com/2017/09/hacking-infusion-pumps.html

48 Ransomware holds data hostage in two German hospitals https://www.scmagazine.com/ransomware-holds-data-

- Cyberattaque à l'origine d'incidents lors de la livraison des repas et de la mise à disposition de conclusions pathologiques[49],
- Disparition d'un disque dur non chiffré contenant les dossiers de près de 30 000 patients[50].

1.3.3. QUI SONT LES ATTAQUANTS

➔ *QUELS SONT LES TYPES DE PIRATE INFORMATIQUE ?*

Nadine Touzeau[51], Net profileuse, à l'instar des profileurs de la police criminelle, a décrit leur personnalité, leur profil psychologique et leurs motivations. À travers son expérience et l'étude de criminels connus, elle décrit, l'univers familial et professionnel de ces criminels.

Les criminels sont des personnalités atypiques selon des références classiques. Nadine Touzeau les classe en grandes catégories, cette distinction permet de mieux connaître son adversaire.

Nous distinguons plusieurs types de pirates informatiques :

1) Les pirates informatiques éthiques qui avertissent les organisations et les utilisateurs en cas de découvertes de failles.
2) Les malveillants, par degré de nuisances :

   - White hat[52] : il est un pirate informatique débutant qui a conscience de ses actes plus ou moins graves. Il agit par impulsion. Ce type de pirate informatique est le plus répondu dans le monde.
   - Grey hat : il est attiré par l'appât du gain ou un acte de vengeance, c'est une personne calculatrice.
   - Black hat : il profite des failles pour effectuer des actes crapuleux en introduisant des virus aux chevaux de Troie, des vers et des logiciels espions dans les organisations. Il est considéré comme un professionnel du cyber crime qui peaufine sa technique et son approche pour atteindre son but, c'est une personne réfléchie.
   - À côté des pirates informatiques cohabitent les « blue hat », consultants en sécurité informatique qui travaillent souvent pour de grandes entreprises, comme Microsoft, pour découvrir des failles éventuelles dans leurs logiciels.

➔ *QU'ELLES SONT LES MOTIVATIONS DES ATTAQUANTS ?*

FINANCIERE (89 % DE TOUTES LES ATTAQUES)

Il est difficile d'estimer, précisément, la valeur marchande des données volées sur le darkweb.

Les sites de revente du darkweb proposent des « *fulz* » (jeu complet de données comme l'adresse, la date d'anniversaire, etc.…[53]). (Voir Annexe n°22 page 211).

Le prix de vente des « fulz » va de 1 euro à 410 euros, le tarif moyen pour l'identité d'une

---

hostage-in-two-german-hospitals/article/528823/

49 Hack attack on a hospital IT system highlights the risk of still running Windows XP http://www.psnews.com.au/qld/490/tech/hack-attack-on-a-hospital-it-system-highlights-the-risk-of-still-running-windows-xp

50 Indiana University Health Arnett Hospital loses USB drive with 29K records https://www.scmagazine.com/indiana-university-health-arnett-hospital-loses-usb-drive-with-29k-records/article/529666/

51 Nadine Touzeau « Net-profiling : analyse comportementale des cybercriminel »

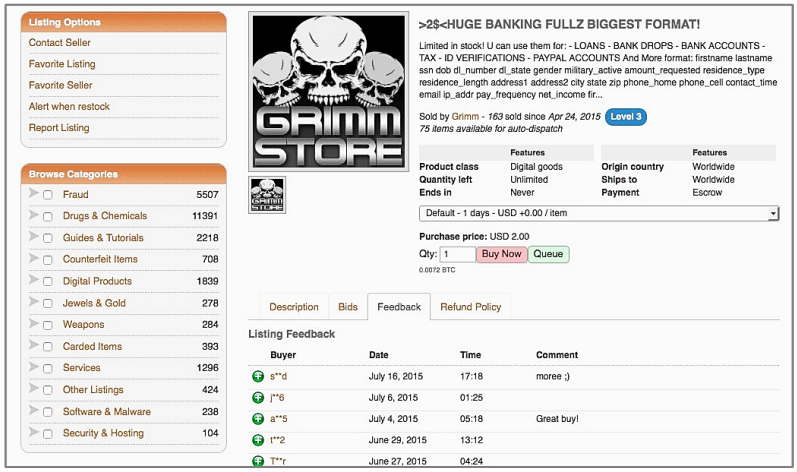
52 Les « *chapeaux* » sont désignés ainsi en référence au shérif, héros de western qui porte un chapeau blanc a contrario des méchants qui portent un chapeau noir.

53 "Here's what your stolen identity goes for on the internet's black market" https://qz.com/460482/heres-what-your-stolen-identity-goes-for-on-the-internets-black-market/

personne est de 19 euros environ.

Des critères supplémentaires rentrent en jeu lorsqu'il s'agit de données bancaires volées. Une identité se négocie jusqu'à 200 euros si, les informations bancaires sont encore valides avec un plafond financier élevé à voler.

Nous accédons à un catalogue, sur le site *AlphaBay*, par exemple, comme chez *Ebay* ou *Amazon.* Il suffit de cliquer sur le bouton « *Fraude* », puis dans des sous-sections telles que « *Informations personnelles et analyses* » ou « *CVV et cartes* » pour filtrer les informations qui nous intéressent et que l'on souhaite acquérir.



ID n° 2 Identités à vendre sur AlphaBay (source qz.com)

ID n° 3 Black Market (source qz.com)

Il est intéressant de voir l'envers du décor et de s'intéresser à la valeur donnée à aux informations par les internautes eux-mêmes. Les internautes estiment la valeur financière pour obtenir leurs données[54] à :

- 2,70 € pour le genre (homme/femme),
- 69,55 € pour un identifiant et mot de passe,

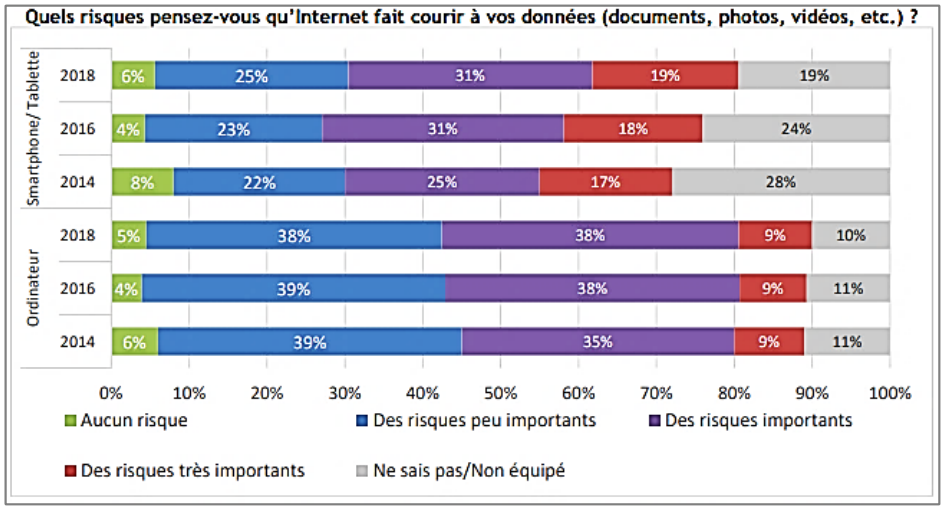
54 L'étude conduite auprès d'un panel de 1 903 personnes issues de différents pays : Allemagne, Belgique, Danemark, Espagne, États-Unis, France, Grèce, Irlande, Italie, Japon, Luxembourg, Pays-Bas, Pologne, Royaume-Uni, Russie, Slovénie, Suède et Suisse par institut Ponemon (https://www.ponemon.org/). https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/reports/rt_privacy_and_security_in_a_connected_life.pdf

- 5,50 € pour un numéro de téléphone et 33,03 € pour les informations bancaires.
- Le plus surprenant, est l'estimation des données de santé à 54,87 € !

La valeur moyenne, des données personnelles dans le monde, est estimée à 17,98 euros.

Les internautes sous estimes le prix de la confidentialité de leurs données, sont inconscients des dangers encourus et malgré tout, pensent qu'internet est fortement dangereux !

La perception des risques sur les données détenues par les internautes (documents, photos, vidéos, etc.) stockées sur les ordinateurs fixes ou portables est relativement stable depuis 2014 :



ID n° 4 CLUSIF 2018 Menaces informatiques et pratiques de sécurité en France page 92

Le récent rapport du CLUSIF indique que 87 % des personnes interrogées jugent qu'il est important de protéger sa vie privée, voire très important pour 48 % d'entre elles et que 68 % estiment qu'Internet met leur vie privée en danger, dont 16 % « fortement » (inchangée depuis 2014).

IDEOLOGIQUE (« HACKTIVISTES »[55], CYBER TERRORISTES, CYBER PATRIOTES),

Les mouvements activistes militent et agissent pour des causes différentes :

- La religion : l'exemple le plus connu est le cyber califat qui œuvrait pour l'état islamique,
- La géopolitique : exemple *IDF team* défend Israël, *The Jester* lance des attaques patriotiques en faveur des États-Unis,
- La censure : ces groupes pratiquent la censure des internautes avec lesquels ils ne sont pas d'accord. Par exemple Hell, hacker Russe, a attaqué des blogueurs, des journalistes et des écrivains russes et *Antileaks* est un groupe d'Hacker qui milite contre *Wikileaks*,

55 L'hacktivisme (contraction d'hacker et activisme), est une forme de militantisme utilisant des compétences du piratage informatique dans le but de favoriser des changements politiques ou sociétaux.

- Le nationaliste chinois : cette forme d'activisme favorise la fortification de l'État chinois, et ceux issus de la culture « hackers » : les *Anonymous*, *Cult of the Dead* Cow[56] et *LulzSec*[57].

Des groupes d'activistes[58] apparaissent comme les *Anonymous en 2003*. Ce groupe interagit avec d'autres groupes comme *Occupy Wall Street*[59] et le mouvement du *15-M1* [60] qui a donné naissance aux *Indignés* en Espagne[61]. Le groupe *X-Net*, hackers et défenseurs du logiciel libre, est également composé anarchistes et fait partie du mouvement altermondialiste.

Les pirates informatiques activistes valorisent une « éthique » antiautoritaire et prônent la désobéissance civile. La vision rageuse d'activisme politique est venue de la culture du *luzl*[62], que l'on pourrait traduire comme « *une euphorie de la transgression* ».

Les mouvements se sont politisés dans les années 1990, lorsque les états ont voté des lois pour les poursuivre. Wikileaks[63] a mis en lumière cette vision des pirates informatiques.

Anonymous est à l'opposé *Wikileaks*, constitué d'un petit groupe de personne. Anonymous est un mouvement participatif, qui mène des actions directes/coup de poing, ne défend ni philosophie ni programme politique. C'est en quelque sorte le reflet « guerrier » de *Wikileaks*.

ÉTATIQUE, ESPIONNAGE,

En France, des milliers de documents internes au parti « En marche » ont été publiés sur internet à la suite d'un piratage du site du parti d'Emmanuel Macron en 2017.

Le porte-parole du mouvement a indiqué que des messageries personnelles et professionnelles avaient été piratées. Neuf gigaoctets de fichiers ont été publiés sur internet en plusieurs lots.

Des pirates informatiques du mouvement les Anonymous, ont attaqué plusieurs sites du gouvernement espagnol en catalogne, le 20 août 2018 afin de protester contre la politique mise en place[64].

Certaines personnes comme Andrés Sepulveda[65] (Colombien), ont pris part dans les campagnes politiques. Utilisés comme mercenaire pour déstabiliser les adversaires, soient en piratant des informations confidentielles ou révélant tel ou tel scandale aux yeux du public.

---

56 Cult of the Dead Cow, ou cDc, est une organisation hacker et un média de masse « Do it yourself » fondée en 1984 à Lubbock, aux États-Unis

57 Lulz Security ou LulzSec est un groupe de hackers à l'origine *grey hat* responsable de plusieurs intrusions informatiques (Sony, CIA)

58 Enid Gabriella Coleman est une anthropologue et chercheure américaine. Ses études portent sur la culture hacker et le cyber militantisme. Spécialiste du collectif Anonymous. Elle est professeure à l'Université McGill. Interview sur Libération « Les hackers se débattent entre l'individu et le collectif » Amaelle Guiton 19/02/2016

59 Occupy Wall Street ou Occupy New York est un mouvement de contestation pacifique, né le 17 septembre 2011, dénonçant les abus du capitalisme financier.

60 Le mouvement des Indignés (Indignados en espagnol) ou Mouvement 15-M1 est un mouvement de manifestations, non violent né sur la Puerta del Sol, en Espagne, à Madrid le 15 mai 2011.

61 Source tempsreel.nouvelobs.com

62 Néologisme anglais « Lulz » est une variante de « lol » (laughing out loud) au pluriel

63 WikiLeaks est une organisation non-gouvernementale fondée par Julian Assange en 2006 dont l'objectif est de publier des documents pour partie confidentiels ainsi que des analyses politiques et sociales à l'échelle mondiale. Source Wikipédia

64 FranceInfo 20/8/2018 : https://www.francetvinfo.fr/monde/espagne/referendum-en-catalogne/espagne-des-hackers-paralysent-les-sites-d-institutions-pour-protester-contre-la-politique-du-gouvernement-en-catalogne_2904117.html

65 Bloomberg Businessweek 31/3/2016 : « Confessions d'un hacker politique en Amérique latine » https://www.bloomberg.com/features/2016-how-to-hack-an-election/

LUDIQUE : ACTION D'ADOLESCENT OU PERSONNE DESŒUVREE

Certains adolescents, souvent très jeunes, pour se venger d'une rebuffade ou de moquerie, pirate le compte Facebook des personnes à l'origine de leur frustration ou agression.

Ils commencent par pirater des sites non sécurisés pour se faire un peu d'argent, afin d'acheter des logiciels « clefs en main ».

Ces jeunes sont surnommés des « *scripts kiddies* », littéralement « *les gamins à scripts* » car ce ne sont pas des génies techniques ni de grands criminels, ils se contentent de petits larcins ou de défis techniques pour épater les amis.

TECHNIQUE

Les cadors des pirates informatiques sont utilisés pour leur haute compétence technique. Leur talent est exploité à des fins politiques ou d'espionnage industriel. Un service « TAO (Tailored Access Operations) » de la NSA (USA) est spécialisé dans cette activité.

Les USA seraient à l'origine d'un programme qui a pénétré les centrales nucléaires iraniennes (Stuxnet) à la fin 2000.

Les autres pays ne sont pas en reste avec la Grande-Bretagne, accompagné des Etats-Unis qui ont développé le programme *Regin*. Ce programme a été utilisé pour infiltrer les institutions européennes avec la complicité, involontaire de la compagnie belge Belgacom.

Les Russes sont également au tableau d'honneur avec la mise sur le marché de leur logiciel espion *Epic Turla*.

Les chinois sont sur la ligne, avec leur unité de développement nommée « unité 61 398 » et de nombreux logiciels d'espionnage envers les états Unis.

PATHOLOGIQUE : ATTAQUE MENEE PAR VENGEANCE OU EMPLOYE INSATISFAIT

Des employés, licenciés ou en conflits avec leur ex-employeur n'hésitent pas à passer à l'acte et à se transformer en hacker. Comme ce Texan (USA) qui a piraté les serveurs de son ancienne société pour commander des IPad, supprimer des données confidentielles et même des données de patients[66].

> « Les mesures techniques qui répondent à un problème humain ont leurs limites » Solange Ghernouati[67]

1.4. PREVISIONS DES CYBER MENACES 2018

Chaque année, les spécialistes de la sécurité diffusent leur analyse de l'année passée et les prévisions de l'année à venir (voir détail Annexe n°3 page 179).

[66] http://www.fredzone.org/licencie-il-pirate-son-ancien-employeur-pour-commander-des-ipad-003

[67] Solange Ghernaouti est professeure à l'université de Lausanne et experte internationale en cybersécurité et cyberdéfense.

Il en ressort les informations suivantes :

- Augmentation des pièces jointes malveillantes de 300 % et des comptes frauduleux sur les réseaux sociaux de 30 % (Proofpoint[68]),
- Risques liés aux crypto monnaies aux attaques menées grâce au machine learning[69], ciblant des secteurs ou activités, comme la supply chain [70]ou le secteur bancaire (Kaspersky[71] et Symantec),
- Danger dû à la transformation digitale, des objets connectés des attaques de phishing et de la méconnaissance des usages de la sécurité sur les ordiphones (ThreatMetrix : Pascal Podvin, Senior Vice-Président Field Operations chez *ThreatMetrix*[72]).

1.5. LES POINTS FORTS ET LES POINTS FAIBLES

1.5.1. LES POINTS FORTS

➔ *TRACES ET LOGS*

Le système d'information est composé, entre autres, de technologies (hardware, software et équipements de télécommunication) qui ont des comportements systématiques, identifiables et pour la plupart prévisibles. Ces outils produisent des traces qui peuvent être exploitées, afin de détecter toute anomalie par rapport à un fonctionnement en condition « normal ».

C'est un atout majeur qui sera utilisé dans le SOC (voir Le SOC (Security Operating Center) ou « Centre d'opérations de sécurité réseau » page 51), qui collecte des données d'activités comme les logs et permet de les analyser.

➔ *INTELLIGENCE ARTIFICIELLE, MACHINE LEARNING ET BIG DATA*

L'intelligence artificielle (IA) fait son apparition dans l'analyse comportementale « déviante ». Celle-ci est couplée à la *Machine Learning*, pour contrecarrer les cybers attaquants et déjouer des tentatives de fraude[73]. Le machine learning permet une pro réactivité dans l'analyse comportementale car cette technologie « apprend » comment détecter automatiquement des comportements anormaux ou inhabituels dans un écosystème de trafic internet crypté, dans le Cloud [74]ou les IOT (Interne des objets).

L'usage du Big Data[75] permet à la Machine Learning et à l'intelligence artificielle d'analyser des millions d'enregistrements, de comprendre et d'apprendre à la manière dont les humains pensent, ce qui serait limité en interne aux seuls enregistrements de l'organisation. Les détections, sont

---

68 Proofpoint est une entreprise spécialisée en cybercriminalité basée à Sunnyvale, California

69 Le Machine Learning est une technologie d'intelligence artificielle permettant aux ordinateurs d'apprendre sans avoir été programmés explicitement à cet effet.

70 La gestion de la chaîne logistique (en abrégé GCL ; en anglais, supply chain management ou SCM)

71 Kaspersky Lab. est une société privée spécialisée dans la sécurité des systèmes d'information fondée par Natalya Kasperskaya et Eugène Kaspersky en 1997 à Moscou, Russie.

72 Spécialiste de l'identité digital https://www.threatmetrix.com/fr/

73 La banque Société générale, par exemple, utilise l'IA et se positionne pro activement face aux attaques de fraudes inconnues

74 Le cloud computing, consiste à exploiter la puissance de calcul ou de stockage de serveurs informatiques distants par l'intermédiaire d'un réseau, généralement Internet (Wikipédia)

75 Le big data, littéralement « grosses données », désigne des ensembles de données devenus si volumineux qu'ils dépassent les capacités humaines d'analyse et même celles des outils informatiques classiques de gestion de base de données ou de l'information. (Wikipédia)

plus rapides, précises et permettent d'écarter les faux positifs[76].

L'intelligence artificielle et le machine learning, en matière de sécurité vont gagner en maturité et seront de plus en plus efficaces. Le rapport Villani, encourage l'utilisation de l'intelligence artificielle dans le cadre de la cyber sécurité, au niveau national et individuel[77], auprès de tous les acteurs économiques nationaux.

1.5.2. LES POINTS FAIBLES

➔ *LES PROJETS*

La notion de protection de l'information est souvent oubliée dans la gestion de projets.

Les bonnes pratiques doivent être appliquées en amont des projets, afin de sensibiliser les parties prenantes et le chef de projet ainsi que les éditeurs de logiciels.

Le RGPD (voir §2.5.1 page 78) est aidant dans cette démarche car il introduit la « *protection des données dès la conception* » et de « *sécurité par défaut* » (*Design by default* et *Privacy by design*).

Les chefs de projets seront mieux armés devant des prestataires indélicats et seront le relais du responsable de la sécurité auprès de prestataires ignorants des dangers que pourraient faire encourir leurs applications à l'organisation.

J'ai été confronté, régulièrement à la méconnaissance des chefs de projets en matière de protection de l'information. Ceux-ci se reposent uniquement sur le RSSI, s'il existe, sous prétexte que cette personne est responsable de la sécurité du système d'information. Il s'agit d'une confusion entre « protection du système d'information » et « protection de l'information » qui regarde l'ensemble des acteurs d'une organisation. Là aussi des campagnes de sensibilisation sont nécessaires afin que le chef de projet soit un véritable partenaire du RSSI et un défenseur des informations de son entreprise.

➔ *LES PRESTATAIRES, LES EDITEURS ET LES CONSTRUCTEURS*

Les éditeurs et les constructeurs déclarent la sécurité comme une de priorité majeure. Cela ne les empêche pas de commercialiser leurs solutions non sécurisées a minima, en plus d'admettre qu'il y a encore plus de risques avec internet et les nouveaux usages.

La sécurité est un enjeu majeur dans le secteur de la santé, le nucléaire, la sécurité nationale… Les constructeurs doivent prendre en compte les problématiques de sécurité dès le début, au lieu de lancer des produits dans le cadre d'une course à l'innovation.

Le RGPD [78] précise que le responsable de traitement, généralement le directeur de l'organisation et le sous-traitant, est considéré comme à égalité en matière de responsabilité vis-à-vis de la protection de l'information. Ce point peut être un levier puissant auprès des partenaires.

Des documents de cadrage et de sécurité doivent être adjoints aux cahiers des charges afin de sélectionner, dès le départ les prestataires qui respecteront les desiderata de la cellule de

---

[76] Un faux positif est le résultat d'une prise de décision dans un choix à deux possibilités (positif et négatif), déclaré positif, là où il est en réalité négatif. (Wikipédia)

[77] Rapport Villani, Focus 5 page 221 « Donner un sens à l'intelligence artificielle pour une stratégie nationale et européenne » Mission parlementaire du 8 septembre 2017 au 8 mars 2018

[78] Règlement européen sur la protection des données https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels

protection de l'information et, mettront tout en œuvre pour protéger les informations de l'organisation.

Les éditeurs doivent s'engager à respecter les chartes et surtout à sécuriser leurs applications de façon professionnelle.

Attention au raccourci dans les choix finaux ! Les failles de sécurité d'un logiciel, d'une infrastructure ou d'un dispositif médical peuvent engendrer d'autres risques, difficilement chiffrables, comme le décès de patients, l'atteinte à l'image et à la réputation d'une organisation, la perte de clientèle, la dévalorisation financière, la perte de propriété intellectuelle ou encore l'augmentation du coût des assurances.

Les éditeurs sont très frileux à se « plier » aux bonnes pratiques. Certains ont le monopole sur des marchés de logiciels ou de matériels, il est difficile de ménager l'organisation, les métiers et les éditeurs et la protection de l'information. Dans ce cas de figure, j'ai été amené à proposer une surcouche logicielle afin de s'assurer que les données personnelles ou de santé étaient protégées a minima, en attendant des évolutions de la part de l'éditeur ou du constructeur. Une grosse pression est exercée par les métiers sur les responsables de la protection de l'information. Des campagnes de sensibilisation sont à mettre en œuvre en prenant ces exemples et des conséquences.

➔ *LES IOT (INTERNET OF THINGS - L'INTERNET DES OBJETS)*

L'explosion des objets connectés (montres Apple ou Androïd, traceur d'activité, surveillance sportive, frigidaire pour conserver des médicaments ou autre produits sanguin, alarme, chauffage, matériel de surveillance médicale mobile, la domotique, certaines alarmes !), très peu sécurisés propose un nouveau terrain de jeux pour les cybers attaquants.

Des études et analyses montrent la prédominance de ces objets sur le marché et auprès des personnes de tout âge. Ces objets sont utilisés à des fins personnelles et professionnelles :

- 30 [79] milliards d'objets seront connectés à internet en 2022 et la totalité des IOT auront plus que doublé (54 %) en 5 ans[80],
- 52 % [81] des Français possèdent au moins un objet connecté et 73 % estiment que la santé est le secteur ou les objets connectés seront le plus utiles.
- 100 % [82] des nouveaux ordiphones seront équipés de technologies biométriques d'ici deux ans, ainsi que les technologies portables (wearable en anglais) et les tablettes à l'horizon 2020.

L'avancée technologique révèle de nouvelles failles de sécurité : la duperie possible des ordiphones, utilisant la méthode de reconnaissance biométrique (image faciale ou empreinte digitale), les comportements humains rentreront aussi en considération :

---

79 Etude de la société Ericsson https://www.ericsson.com/assets/local/mobility-report/documents/2017/ericsson-mobility-report-june-2017.pdf

80 Etude réalisée en août 2017 par le cabinet Gartner https://www.gartner.com/newsroom/id/3790965,

81 Baromètre OpinionWay pour Distreeconnect–LK Conseil de mars 2017, https://www.opinion-way.com/fr/sondage-d-opinion/sondages-publies/opinionway-pour-distreeconnect-2017-les-francais-et-les-objets-econnectes-mars-2017/download.html

82 Cabinet Acuity Market Intelligence, entreprise d'analyse axée sur l'identité. http://acuity-mi.com/

« Par méconnaissance des dangers ou négligence, les utilisateurs modifient rarement le mot de passe par défaut de ces nouveaux outils, dont le mode d'emploi est largement diffusé sur internet », Nicolas Sterckmans83.

Les revenus générés par la biométrie intégrée dans les appareils mobiles (authentification de transaction, applications biométriques) sont de 6,5 milliards en 2016 et devraient atteindre 50,6 milliards en 2022, selon le cabinet Acuity Market Intelligence.

Donc, nous pouvons faire confiance aux fabricants de ces objets quant à l'intérêt de leur chiffre d'affaires avant la sécurisation de leurs produits.

➔ *LES DISPOSITIFS MEDICAUX*

Les hôpitaux utilisent de nombreux appareils connectés à Internet, notamment des équipements biomédicaux hautement spécialisés, ainsi que des ordinateurs pour le personnel et un nombre croissant d'appareils mobiles (accès au dossier patient à partir de tablettes, ordiphone ou TMM - Terminaux Multi Média- installés dans la chambre des patients et connectés sur une prise réseau reliée au système d'information de l'organisation) (voir Annexe n°6 page 182).

Une seule entité BIO-DSI !

Un paradoxe apparaît : les appareils biomédicaux sont des outils informatisés et pourtant ceux-ci sont traités en dehors des services informatiques.

Il est temps de se poser les bonnes questions et de créer une seule entité *BIO-DSI*. Cette dernière plus avancée en matière de protection de l'information, pourra faire bénéficier de son savoir et ses pratiques la partie biomédicale.

Une autre approche est l'expérimentation d'un partenariat interservices. Un membre de chaque service Biomédical-DSI, joue dans une série d'un genre « *vis ma vie* », afin que chaque « *camp* » comprenne les problématiques, le quotidien de l'autre « *camp* » et instaure un dialogue et des pratiques communes.

La formation des ingénieurs biomédicaux est à revoir sur la partie protection de l'information

Les cursus d'ingénieurs biomédicaux doivent inclure un thème « *protection de l'information* », ce qui n'est pas le cas actuellement si l'on se réfère à l'EHESP (école des Hautes études en Santé Publique).

Cette école, de référence, propose un « *master spécialisé équipements biomédicaux* » dont les enseignements principaux sont : « la direction des équipes biomédicales, l'orientation stratégique des établissements de soins, le conseil à l'achat des nouveaux équipements, la gestion du parc d'équipements et les coopérations en matière de recherche… ».

Cette situation créée des tensions, des incompréhensions entre les services DSI et BIO et génère des comportements d'insécurité sur certains appareils, qui doivent malgré tout, être connectés sur le système d'information (accès au dossier patient par exemple).

---

83 Expert en cybersécurité chez l'éditeur de logiciels de sécurité Malware bytes

➔ *LE COMPORTEMENT HUMAIN (SOURCE DE FAILLES)*

LES ETATS

La cybercriminalité est utilisée à des fins politiques pour diffuser de fausses nouvelles, piller des informations au bénéfice de parti politique ou pays adverses.

Le gouvernement a pris conscience de ce « contre » pouvoir et à renforcer l'ANSSI dans la lutte contre ces criminels (voir exemple en Annexe n°5 page 181).

LES ORGANISATIONS

Les organisations ont pris conscience de l'activisme cybercriminel et souscrivent une assurance spécialisée. La compagnie d'assurances *Hiscox* a révélé que 57 % des 3 000 entreprises consultées, aux Etats-Unis, au Royaume Uni et en France avaient été la cible de cyber attaque[84]. L'évaluation des dégâts économiques globaux est estimée entre 375 à 575 milliards de dollars.

Il est à noter que les failles, dues à des comportements humains indélicats ou dangereux sont plus rapidement détectées et éradiquées que les failles dues à des piratages (voir Annexe n°4 page 180).

a) Les organisations organisent leur sécurité après avoir subi une attaque.

En 2017, les mesures les plus populaires étaient le cryptage (51 %), les programmes de formation et de sensibilisation (48 %), la certification ou l'audit de sécurité (39 %) et les systèmes de sécurité tels que SIEM (34 %).

70 % des sondés ont conclu que la menace interne était due au manque d'expertise. Pour 55 %, elle est liée au manque d'implication des directions et de responsabilisation. Mais 60 % des sondées ont indiqué ne pas exiger que les employés suivent à nouveau des formations à la sécurité à la suite d'un incident.

b) Maturité de la prise de conscience du danger ?

La Direction générale, en grande majorité affirme se préoccuper de la cyber sécurité et, contradictoirement, ce point arrive en cinquième position des risques importants à gérer.[85]

Les organisations (31 %) positionnent la cyber sécurité dans leurs dix premières préoccupations[86].

Une des personnes clef en matière de maturité du risque dans l'organisation est le RSSI. Il apportera son éclairage, nécessaire à prise de conscience de la cyber sécurité, auprès de la Direction. Sans cette action, il lui sera très difficile d'obtenir un appui fort auprès de l'ensemble

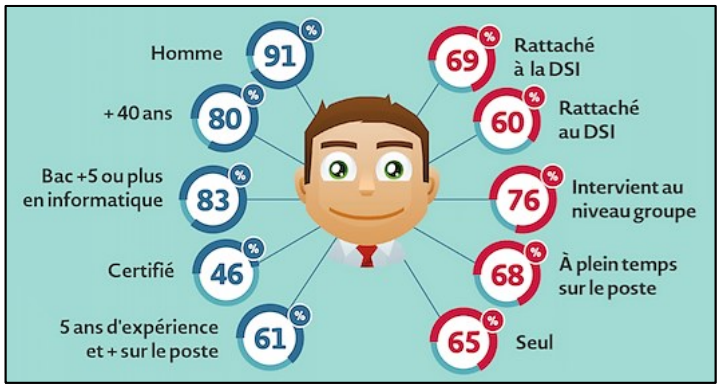
---

84 Livre blanc : https://blog.hiscox.fr/pdf/livreblanc-ecommerce.pdf

85 Enquête annuelle « *Building Trust* » de KPMG.
En 2016, 83 % des PDG avaient indiqué que la réduction des risques cyber fait partie de leur rôle, ils ne sont plus que 72 % à l'affirmer en 2017 ! http://itsocial.fr/metiers/direction-generale/pdg-ont-chemin-a-faire-de-prendre-cybersecurite-serieux/

86 Le « Guide de la cybersécurité 2016 Alliancy Etude Deloitte » révèle que 83% des entreprises se considèrent comme exposées aux cyberattaques dont 25% très exposées, mais, que 31% seulement place la cybersécurité dans leurs dix premières préoccupations pour leur organisation. CESIN (Club des Experts de la Sécurité de l'Information et du Numérique). 36% des organisations estimaient placer la gouvernance de la cybersécurité, dans leur organisation, au bon niveau, 20% indiquaient qu'il valait mieux former les collaborateurs aux questions de la cybersécurité (soit 63% de mois par rapport à 2016) et seulement 11% avaient d'intention d'adapter les solutions en place à la transformation numérique (soit 40% de moins que 2016)

des personnes de l'organisation[87].



ID n° 5 CESIN - Qui est le RSSI ?

La cyber sécurité manque de résonance au sein des organisations, qui placent leurs clients et leurs collaborateurs face à des risques non maîtrisés.

La moitié des organisations interrogées en 2016, n'ont pas de centre de supervision et d'administration de la sécurité, ni de veille sur les cybers menaces ou d'abonnement à des programmes d'identification des vulnérabilités.[88]. Ce constat peut remettre en cause la survie de leur organisation. Les écosystèmes s'agrandissent, se modifient, il sera de plus en plus difficile de superviser l'ensemble des dispositifs, si rien n'est fait dès à présent.

Il convient de se poser les bonnes questions :
Veut-on que son organisation résiste aux cyberattaques ?
Veut-on que les collaborateurs soient un des premiers vecteurs de contamination de l'organisation du fait de son ignorance ?

Ce constat laisse songeur quant aux beaux jours accordés au cyber attaquants, en tout genre, par les organisations.

c) *Les investissements*

Les organisations sous-estiment l'investissement nécessaire pour protéger leur système d'information. Une estimation de 5 % à 10 % est préconisée par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information).

L'ENISA[89] a mené des études afin d'évaluer les coûts exacts de cyberattaque sur les entreprises. Malheureusement, il est très difficile de dégager une vue unique, en tenant compte des nombreuses variables et de méthodes métriques utilisées[90]. Un ratio risques/investissement est difficile à

---

87 Le magazine « *Alliancy le mag* » a mené une enquête auprès de 80 acteurs de la sécurité des systèmes d'information. Dans l'ordre, les acteurs les plus matures sont le RSSI (68%), la direction (52%) et le reste de l'équipe (46%).

88 Enquête réalisée par le cabinet Ernst & Young Global Limited entre juin et août 2016 auprès de 1735 professionnels de la sécurité de l'information et de l'IT issus des plus grandes organisations du monde. 44% des répondants n'ont pas de SOC, 64% n'ont pas de stratégie de veille des cybers menaces, ou seulement informelle, 55% n'ont pas de programme d'identification des vulnérabilités, ou seulement informelle.

89 L'Agence européenne chargée de la sécurité des réseaux et de l'information (AESRI) (ENISA selon l'acronyme en anglais) est une agence de l'Union européenne créée le 10 mars 2004 par un règlement de l'Union européenne.

90 https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis/at_download/fullReport

dégager (voir §4.4 page 136).

L'enjeu est de revoir la gouvernance de la cybersécurité pour mieux agir

d) La cyber sécurité est une action prioritaire. Si elle est considérée comme un fardeau, cela se reflétera en interne dans toute l'organisation.

Ce message devrait être porté par la direction et communiqué à tout le personnel.

La cyber sécurité devrait être intégrée à la culture de l'organisation dans le cadre de ses activités ; cela permettrait d'envoyer le bon message selon lequel l'intégrité, la confidentialité et la sécurité des données sont importantes et ne doivent pas être prises à la légère et découragerait des activités non autorisées par les acteurs de l'organisation.

L'HOMME AU CENTRE DE TOUS LES DANGERS

En avril 2017, *Médiamétrie* dénombrait plus de 45,1 millions d'internautes en France, soit une majorité d'êtres humains faillibles, inconscients ou ignorants devant Internet et ses peuplades parfois hostiles !

Nous avons changé d'océan et naviguons entourés de pirates, qui tel Rackham le Rouge[91], abordant notre ordinateur lorsque nous surfons sur internet.

Les quelques chiffres suivants justifient l'importance de prendre en compte les acteurs de l'organisation et déborder, lorsque cela est possible, à la sphère privée.

Éric Jardine chercheur au Centre pour l'innovation dans la gouvernance internationale (CIGI)[92] indique que « *le point faible de la plupart des systèmes de sécurité informatique est souvent l'utilisateur individuel, et non pas le système lui-même* ».

Il est prouvé que 84 % des risques d'infection du système d'information d'une organisation sont dus aux utilisateurs du système d'information. [93],

Les dangers les plus fréquents (95 %) sont dus à l'ouverture de courriel piégé (qui représente 70 % des attaques), et aux mots de passe non sécurisés. Les mots de passe les plus utilisés sont « *123456* » ou « password » ![94]

La même étude révèle que, 51 % des organisations considèrent que les erreurs humaines sont à l'origine des plus grandes pertes financières, en termes de coût. Malgré ce constat, seulement 13 % avouent que leur priorité est de se protéger des erreurs humaines dans l'organisation à l'origines de catastrophes financières.

---

91 John Rackham (dit Jack), plus connu sous le nom de Calico Jack, est un pirate du XVIIIe siècle. Il doit son surnom aux vêtements très colorés faits de calicots qu'il portait. Il est surtout connu parce qu'il comptait parmi les membres de son équipage les deux plus célèbres femmes pirates : Anne Bonny et Mary Read. Source wikipédia

92 Le CIGI a pour mission de mener des recherches et des analyses de calibre mondial, et de sensibiliser les décideurs à l'innovation. https://www.cigionline.org/about

93 Etude eCSI lors du Gartner Identity & Access Management Summit 2014, à San Francisco ; menée auprès de 300 participants

94 Source https://blog.econocom.com/

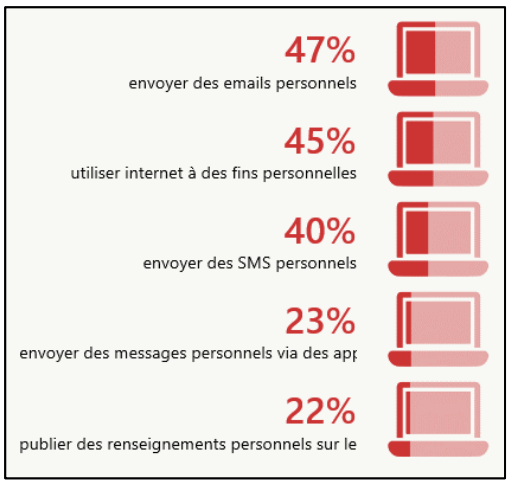
Voici le décor planté ! L'humain est le centre du sujet de la cyber sécurité, ou devrait l'être !

Plus de 50 % des incidents de sécurité, volontaires ou malintentionnés sont dus à des origines internes aux organisations[95]. Ceux-ci sont perpétrés pour un tiers par des employés en place ou, qui ont quitté l'organisation, et le restant par des prestataires en place ou anciens ainsi que des fournisseurs ou partenaires. [96]

Les employés adoptent des raisonnements contradictoires : plus de la moitié (55 %) affirme que le matériel professionnel peut être utilisé à des fins personnelles sans nuire à l'organisation[97], et parallèlement 46 % des mêmes employés ne savent pas quelle attitude adopter pour se protéger des techniques d'ingénierie sociale et ne connaissent même pas cette expression !

Les personnels interrogés indiquent, à 98 %, que leurs données personnelles sont importantes. Toutefois 60 % d'entre eux déclarent avoir commis des actions pouvant compromettre ces données, sur des outils mis à disposition par l'organisation à usage professionnel !

Parmi les actions dangereuses les employés déclarent, à :



ID n° 6 Enquête effectuée par kCura « Big Data From Employees Leads to Big Risk for Employers »

Les pratiques des employés mettent en danger la protection des informations lorsque, les politiques de sécurité mises en place, sont ignorées. Ces politiques existent, la plupart du temps, et portées à la connaissance des membres de l'organisation ; même si les acteurs de l'organisation disent, haut et fort (63 %), qu'ils n'en ont pas connaissance, ou bien qu'elles n'existent pas (56 %).

4 milliards d'internautes dans le monde, 3,2 milliards sur les réseaux sociaux, 11 nouveaux utilisateurs de réseau social chaque seconde

Les réseaux sociaux, sont la cible favorite des pratiquants de l'ingénierie sociale. Ces sites sont des mines d'or d'informations pour connaître les employés de l'entreprise, leurs agissements, leur vie, leur déplacement et leur fonction dans l'entreprise.

Les pratiquants passent environ 6 heures par jour connecté, soit un tiers du temps hors les périodes de sommeil. « *L'ingénierie sociale est la première cause des fraudes et d'introduction dans les réseaux d'entreprise* », indique Gérôme Billois, senior manager cyber sécurité chez Wavestone[98].

---

95 Enquête IBM Cyber Security Intelligence https://www.slideshare.net/ibmsecurity/key-findings-from-the-2015-ibm-cyber-security-intelligence-index. En 2015, 60% des incidentes sécurités relevés (sur 52 885 311), sont dus à des origines internes aux organisations (15,5% d'attaques involontaires et 44,5% d'attaques malintentionnées) et seulement 40% d'origines externes aux organisations

96 Enquête menée par PMW, en 2015, « The global state of information Security survey ». Les incidents de sécurité sont dus à 34% à des employés de l'organisation, 29% à d'anciens employés, 22% à des prestataires de services, 19% à d'anciens prestataires de service et 16% à des fournisseurs ou partenaires

97 Enquête « Big Data From Employees Leads to Big Risk for Employers » effectuée par kCura.

98 Wavestone est un cabinet de conseil spécialiste de la transformation des entreprises réputé.

Au-delà de ce déballage médiatique, les pratiques des employés, mettent en péril les informations de l'organisation. Les employés contournent les règles, utilisent leur messagerie comme lieu de stockage et de classement, pour 70 % des cas, en lieu et place où en plus du logiciel sécurisé prévu à cet effet.

Que fait la DSI ?

Le vol **d'ordinateurs non sécurisés** et, utilisés pour le traitement de **données sensibles** peut être dramatique comme la divulgation de données de médicales à la vue du monde entier.

ID n° 7 pertes de données médicales. Source CB News

Les sous-marins pirates informatiques dans l'organisation !

La moitié (51 %)[99] des employés indique qu'ils seraient prêts à pirater leur organisation ou d'autres entreprises, avec toutefois, l'appréhension de se faire prendre, la « *souris dans le sac* ».

L'intérêt est, le plus souvent, personnel comme, par exemple :

- Augmenter son nombre de jours de congé (23 %),
- Transférer des fonds sur son propre compte bancaire (23 %),
- Faire du shopping en ligne sans rien débourser (20 %)
- Rembourser son emprunt (14 %).
- Les motivations, pour certains, sont plus de l'ordre « *politique* ». Ces personnes souhaiteraient :
- Bloquer les activités de certaines organisations immorales (14 %),
- Rechercher des renseignements nationaux confidentiels (11 %)
- Modifier certaines lois (5 %).

[99] L'organisation anglaise *CyberArk*[99], spécialiste des cyberattaques a réalisé une enquête auprès de 1000 employés de bureau britanniques dans des organisations de plus de 250 salariés. https://www.cyberark.com

Voici les résultats d'une enquête menée par *Intermédia*[100], afin de comprendre à quel point il est important de s'intéresser aux employés :

- Sur les 1 000 employés de bureau interrogés, 24 % utilisent les mêmes identifiants de connexion dans le cadre de leur travail et pour leurs comptes personnels et 42 % des professionnels de l'informatique utilisent les mêmes mots de passe !
- 96 % des employés, enregistrent leurs mots de passe sur leur ordinateur de travail sécurisé,
- 57 %, soient plus de la moitié des employés de bureau interrogés admettent qu'ils stockent des fichiers de travail sur leur bureau ou dans des dossiers du bureau. La plupart des organisations n'ont pas de programme de sauvegarde des fichiers enregistrés localement sur les ordinateurs des employés. Sur le bureau, les fichiers sont encore plus visibles et accessibles rapidement par une personne malveillante,
- 34 % des employés, interrogés, utilisent des plateformes de partage personnelles à des fins professionnelles (exemple : Dropbox, Icloud…). Ils déposent des documents confidentiels de leur entreprise. Cette pratique est en hausse de 12 % par rapport à 2015.
- 23 % des employés sauvegardent leurs documents professionnels sur leur ordinateur personnel à la maison. Cette machine est souvent en multiservice familiale, peu sécurisée. 64 % d'entre eux s'adressent les documents professionnels sur leur messagerie personnelle.

Les constats et enquêtes ci-dessus démontrent que l'homme est bien au centre de tous les dangers. Ils adoptent des attitudes dangereuses et inconscientes vis-à-vis de son organisation, s'appropriant, à des fins personnelles, les outils et matériels mis à disposition à des fins professionnelles. Il a même des pensées criminelles !

Les acteurs sont beaucoup plus prudents lorsqu'il s'agit de leur vie privée et de l'usage de leur matériel personnel. La méfiance des appareils mobiles (ordiphone et tablette) est présente et est rarement utilisée pour effectuer des achats sur Internet. La moitié des personnes interrogées refusent, même d'utiliser ce genre d'équipement pour le shopping sur internet[101]. 68 % des personnes interrogées considèrent qu'Internet met leur vie privée en danger (16 % fortement), ce qui ne les motive pas, pour autant, à modifier régulièrement leur accès sur les réseaux sociaux ou de protéger leur équipement informatique ou mobile.

LA GENERATION X, Y ET Z

a) Qui sont-ils ?

La génération « S » ou « baby-boomer », est née à la fin ou après la dernière guerre mondiale.

Les enfants des « baby-boomers » sont nés entre 1965 et 1979, et sont nommés la génération « X ».

Maintenant on parle de la génération « Y » née entre 1980 et 1995. Ils sont parfois surnommés les « WHY » à cause de la prononciation de la lettre Y en anglais.

On nomme, les jeunes gens nés autour de 1996, la génération Z ou génération Google.

---

100 https://www.intermedia.net/report/datavulnerability2017-part3

101 Enquête 2018 du CLUSIF sur la « Menaces informatiques et pratiques de sécurité en France ».

b) La génération X

Ces individus sont respectueux de la hiérarchie et font confiance à leur entreprise, à laquelle ils sont attachés.

La règle et les processus ont été mis en place par eux au sein des organisations.

Ces parents ont laissé beaucoup de place à la communication et au partage à leurs enfants (les Z), Françoise Dolto, est, en partie à l'origine de ces changements sociologiques.

c) La génération Y en entreprise

La génération Y représentera 75 % de la population active en 2025, et devrait représenter 50 % de la main-d'œuvre mondiale en 2020.

La génération des 20 à 35 ans représente un travailleur sur 3 aux Etats-Unis[102].

Cette génération a un rapport différent avec l'autorité qui, si elle n'est pas compétente ne sera pas respectée. Ils peuvent rentrer facilement en compétition avec leurs collègues, communiquent facilement à l'aide des technologies ou en face-à-face. Cette génération place le travail en équilibre avec la vie familiale et cherche une certaine qualité de vie.

Ce sont des individus qui pensent à court terme, sont très mobiles et favorisent la reconnaissance de leurs compétences. Ils n'hésitent pas à bouleverser les règles, à vérifier et compléter les informations qui leur sont fournies.

La génération Y est tombée dans la « *marmite de la révolution internet* ». Elle a grandi dans une société ou l'ordinateur personnel, le jeu vidéo et l'Internet qui ont pris de l'importance et sont devenus accessibles.

Elle appréhende la technologie intuitivement, par expérimentation et est qualifiée de « *digitales natives* »[103]. Ces individus évoluent parmi des flux d'information constants et accessibles immédiatement. « *La communication paroxystique, mobilité incessante, information instantanée est dans l'ADN des Y* » [104].

d) Qu'elle est l'usage de la technologie par les « Y » ?

Globalement la génération Y, pense détenir assez de connaissance en matière de sécurité de l'information, alors même que leur pratique est jugée à risques : [105]

- Utilisation d'équipements personnels pour augmenter leur productivité,
- Téléchargement, pour 25 %, de fichiers d'organisations ou d'applications tierces sur leurs terminaux personnels sans prévenir leur responsable informatique,

---

102 Le Pew Research Center est un centre de recherche (think tank) américain qui fournit des statistiques et des informations sociales sous forme de démographie, sondage d'opinion, analyse de contenu. Son siège social est à Washington, D.C.

103 Un enfant du numérique ou « digital nativ » est une personne ayant grandi dans un environnement numérique. Source Wikipédia

104 Myrial Levain et Julia Tissier, La Génération Y par elle-même, quand les 18-30 ans réinventent leur vie, François Bourin Editeur, 2012.

105 Forcepoint, éditeur leader en cybersécurité, publie les résultats d'une enquête sur l'utilisation de la technologie par la Génération Y effectuée auprès de 670 personnes, nées entre 1977 et 1994.

- Utilisation de mots de passe forts, mais identiques dans plusieurs systèmes et applications et même après une mauvaise expérience,
- Connexion à des réseaux Wifi public non protégés,
- Stockage des fichiers professionnels dans un Cloud personnel,
- Installation d'applications sur leur poste de travail, sans l'approbation de la DSI.

e) *Que dire de la génération Z, futurs employés ?*

Les « Z » sont nés avec le numérique, le Web 2.0 [106], n'ont jamais connu un monde sans Internet et baignent dans une culture globalisée et collaborative. Ils sont surnommés, également, la génération C (pour Communication, Collaboration, Connexion et Créativité).

Ils maîtrisent les outils informatiques (ordinateurs, GPS, ordiphones, tablettes), les utilisent au quotidien et ne peuvent pas vivre sans. Les enfants de la génération « Y », eux, ont vécu leur enfance et adolescence sans ces nouvelles technologies.

Les moins de 20 ans représentent, aujourd'hui, 16 millions de personnes. Les organisations doivent s'y préparer dès maintenant. La légitimité de la hiérarchie s'évaluera par la confiance qu'elle accordera aux collaborateurs, à être à l'écoute et à fédérer autour de projets inspirants.

Les « Z » sont des individus hyperconnectés, ils évoluent dans un écosystème en interaction permanente. Ils amèneront cet usage des technologies dans les organisations. Les responsables devront s'adapter, moduler leur action et leurs discours pour leur faire comprendre les dangers d'internet tout en leur permettant d'accéder au monde !

Le côté positif de cette génération est une forte envie d'apprendre et d'expérimenter. Ils ont l'expérience des MOOC et des tutoriels sur YouTube. Ils sont pragmatiques et savent surfer intelligemment sur la toile.

f) *En résumé qui sont ces générations et comme les appréhender vis-à-vis de la sécurité ?*[107]

GENERATION X	GENERATION Y	GENERATION Z
VERTICAL 	CENTRAL 	HORIZONTAL 
Individu qui s'inscrit dans une perspective commune de l'entreprise	Individu au centre de « ses » préoccupations	Individus positionnés dans une logique transverse en entreprise, dans sa vie personnelle et aux quatre coins du monde.
Confiance dans l'entreprise Respecte la hiérarchie et les règles	Première génération « mondiale » Comportement à risques (mot de passe, données sur le cloud non sécurisé, wifi publique) Profite de la vie au présent. Est dans l'instantané et la simultané	Hyperconnectés, Usage intensif des réseaux Maîtrisent les technologies Curieux, utilisent internet avec prudence

ID n° 8 résumé qui sont ces générations X, Y et Z

---

[106] L'expression « Web 2.0 » désigne l'ensemble des techniques, des fonctionnalités et des usages qui ont suivi la forme originelle du web, www ou World Wide Web, caractérisée par plus de simplicité et d'interactivité (sociabilité). Wikipédia

[107] BNP Paribas et The Boson Project publient l'étude « *La Grande InvaZion* », une enquête réalisée auprès de 3 200 jeunes français de 15 à 20 ans. https://cdn-actus.bnpparibas.com/files/upload/2015/01/20/docs/lagrandeinvazionbnpparibastbpweb.pdf, 21/05/2015

g) *Y a-t-il un RSSI dans l'entreprise ?*

Les réponses analysées dans l'étude, mentionnée ci-dessus, démontrent, qu'il n'y a rien de spécifiquement prévu pour accueillir ces nouvelles générations. Les adaptations se font au cas par cas, en assouplissant les règles de, présence (flexibilité des horaires), d'usage d'appareils mobiles et la révision des programmes de sensibilisation (usage du BYOD[108] et ses dangers, production sécurisée).

La génération Y a perdu la notion du réel, sur internet. On la considère, à tort, comme un groupe d'individus armés, car hyperconnectés.

La génération suivante, est plus prudente car elle est informée par l'entourage familial, l'école, les médias, elle se fait plus discrète sur les réseaux sociaux et utilise des pseudonymes.

Faut-il ouvrir l'accès aux réseaux sociaux dans l'entreprise ?

h) *Les réseaux sociaux sont synonymes de dangers et sont un foyer d'infection :*

- Twitter a été infecté par un virus en 2016[109],
- Facebook ou LinkedIn ont vu se propager une photo infectée. L'internaute cliquait sur la photo reçue et était redirigé vers une copie du site YouTube où était proposée l'installation d'un programme pour pouvoir visionner une vidéo[110],
- Instagram a été piraté par des pirates informatiques russes, qui étaient parvenus à dissimuler un malware dans des commentaires postés sur le réseau social. Le virus était dissimulé dans le commentaire afin de mener l'internaute vers un site qui infecterait son ordiphone[111],

Les jeunes employés de la Silicon Valley, à 67 %, n'utilisent pas l'outil institutionnel pour joindre leurs collègues dans le cadre de leur travail, mais Facebook, dans le pire des cas, ou d'autres moyens comme WhatsApp.

Cette génération est tellement imprégnée par les réseaux sociaux, que 60 % des 18 à 34 ans ne souhaitent pas travailler dans une entreprise interdisant l'usage des réseaux sociaux sur le lieu de travail.

Le Responsable de la Sécurité du Système d'Information à fort à faire avec la génération « Y » qui est persuadée que la cyber sécurité est seule du ressort de « l'informatique » il devra, dès à présent, réfléchir aux futures actions de sensibilisation des « Z ».

---

[108] BYOD, abréviation de l'anglais « bring your own device », en français, PAP pour « prenez vos appareils personnels » ou AVEC pour « apportez votre équipement personnel de communication », est une pratique qui consiste à utiliser ses équipements personnels dans un contexte professionnel.

[109] Le réseau social Twitter infecté par un malware http://www.lepoint.fr/high-tech-internet/le-reseau-social-twitter-infecte-par-un-malware-25-08-2016-2063647_47.php, 25/08/2016

[110] wooxo https://www.wooxo.fr/Wooxo-news/Le-blog-Wooxo/virus-reseaux-sociaux, 28/11/2016

[111] journal geeko.lesoir.be http://geeko.lesoir.be/2017/06/10/un-virus-circule-sur-instagram/, 10/06/2017

➔ *LES PROFESSIONNELS INFORMATIQUES*

Les **professionnels des services informatiques sont davantage impliqués que leurs collègues dans des comportements à risque**[112]. Certains professionnels du système d'information (28 %) reconnaissent avoir accédé au système d'un ancien employeur et pourraient (31 %) infiltrer leur organisation, s'ils pouvaient en tirer quelques bénéfices personnels.

Les profils techniques sont les plus enclins à pratiquer ces méthodes car ils savent contourner les contrôles mis en place, avec une inconsciente totale de la sécurité de leur organisation.

C'est pourquoi, il est important d'appliquer de bonnes pratiques (comme d'identifier les fonctions, séparer les rôles, la gestion des accès et habilitations aux points sensibles dans la DSI), et de responsabiliser et sensibiliser ces techniciens par des professionnels en cyber sécurité. Ces personnes auront l'impression d'être admises dans *LE* cercle de « cyber espion » ou « cyberdéfense » et seront les premiers à semer la bonne parole, avec une certaine autorité « *je sais, donc je suis !* ».

L'ANSSI intervient régulièrement dans des réunions « cyber sécurité » ou des formations organisées, dans leurs locaux. Des spécialistes font la démonstration de piratage de badges, de téléphones portables… En direct.

1.6. LES MENACES OU TYPES D'ATTAQUES

1.6.1. LES TYPES D'ATTAQUES ET MENACES

On distingue plusieurs types d'attaques (voir le détail en Annexe n°29 page 215) :

TYPE D'ATTAQUE	EXPLICATION
Ver	Un ver est un programme qui se propage d'ordinateur à ordinateur par l'Internet et fonctionne à l'insu de l'utilisateur. Le ver ne s'introduit pas au dans un autre programme comme le virus.
Virus	Un virus est un logiciel qui se propage par les réseaux ou les supports amovibles (exemple clef USB), infecte les programmes en les parasitant et donne toute sa puissance lorsque ce programme est lancé en créant des dégâts, tout ça à l'insu de l'utilisateur. Les antivirus agissent a posteriori, c'est pourquoi les utilisateurs doivent être vigilants aux messages qui sont délivrés dans leur boîte aux lettres.
Rançongiciel ou ransomware	Le ransomware consiste à s'infiltrer sur un système d'information (généralement au travers de courriels frauduleux), puis à en chiffrer tous les fichiers, et enfin, à exiger une rançon à payer en bitcoins. Les hôpitaux en font tout particulièrement les frais, et choisissent souvent de payer plutôt que de rester paralysés.
DDoS (Distributed Denial of Service) déni de service distribué.	Il s'agit d'une attaque informatique à l'origine de plusieurs sources produisant une indisponibilité d'un service.

ID n° 9 les malwares

[112] Source Intermedia's 2015 Insider Risk Report https://www.intermedia.net/resource/intermedias-2015-insider-risks-report-survey-results, août 2015. 32 % des informaticiens déclarent avoir partagé leurs identifiants et mots de passe avec d'autres employés, ce taux plafonne à 19 % pour tous les répondants confondus.

➔ *ATTAQUES ET VULNERABILITES HUMAINES*

Dès 2006, le député Pierre Lasbordes indiquait dans son rapport « *La Sécurité des systèmes d'information - Un enjeu majeur pour la France* »[113] que les vulnérabilités humaines peuvent être liées à des incidents de sécurité dans les organisations.

Les mêmes constats étaient déjà listés comme le manque de sensibilisation des acteurs de l'organisation et leur inconscience, le Shadows IT [114]et une mauvaise utilisation d'internet[115].

Dans la typologie des menaces, le facteur humain est essentiel et se matérialise sous plusieurs formes (voir détails Annexe n°30 page 216) :

TYPE D'ATTAQUE	EXPLICATION
L'ingénierie sociale **Compromission de la messagerie en entreprise (BEC, Business Courriel Compromise)** **L'arnaque au président ou escroquerie aux faux ordres de virement (FOVI)**	Afin de contourner des systèmes de protection, ou d'obtenir des informations normalement confidentielles, un attaquant peut tenter d'abuser de la naïveté d'un utilisateur peu sensibilisé.
La manipulation d'individus	MICE (Money, Ideology, Compromise, Ego). Cet acronyme anglophone résume les différents moyens pouvant permettre de s'assurer le concours de quelqu'un. Qu'il soit attiré par l'argent, une idéologie commune (religieuse ou politique), sous l'emprise d'une compromission ou de son ego, un individu peut être manipulé.
Vol d'information **Phishing** **Vishing**	Les attaquants essaient de duper les employés à l'aide de courriers électroniques.
Longlining	Courriels frauduleux personnalisés inspirés par des campagnes marketing. Ces messages passent à travers les antispams (antipourriel) ou analyse de contenu et ne contiennent pas de pièce jointe.
Attaque « Watering Hole » (ou « point d'eau »)	Il s'agit de compromettre des sites web stratégiques et d'y attirer, par la ruse ou des courriels, certaines personnes qui seraient intéressées par les informations diffusées, comme une oasis, mais sans eau !
Money muling	Il s'agit de blanchiment d'argent. Un malfrat vole de l'argent ou des biens par l'intermédiaire de malware ou hameçonnage, de trafic de stupéfiant et recrute, habilement, des internautes pour transférer cet argent via leur compte bancaire et contre rétribution.[116]
Pourriel vocal ou Ping call	Notre téléphone sonne une seule fois et cela raccroche. L'escroc espère que vous rappeliez ce correspondant car il s'agit d'un numéro de téléphone surtaxé. Cela arrive sur les portables et les lignes fixent.
SMS frauduleux	Le but est le même que le Ping Call, allécher le propriétaire d'ordiphone à répondre au numéro indiqué, par un message alléchant (exemple : Nous avons gagné au loto). Certains escrocs rentabilisent leur investissement en revendant des

113 Source https://www.ladocumentationfrancaise.fr/rapports-publics/064000048/index.shtml

114 Shadow IT est un terme fréquemment utilisé pour désigner des systèmes d'information et de communication réalisés et mis en œuvre au sein d'organisations sans approbation de la direction des systèmes d'information. Source Wikipédia

115 Rapport « La Sécurité des systèmes d'information - Un enjeu majeur pour la France » rédigé par le député Pierre Lasbordes, 13/01/2006, http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/064000048.pdf, page 43

116 Police Nationale : https://www.police-nationale.interieur.gouv.fr/Actualites/Dossiers/Cybercrime/Money-muling-ne-vous-mettez-pas-dans-de-beaux-draps, 28 novembre 2017

TYPE D'ATTAQUE	EXPLICATION
	numéros de téléphone de personnes qui ont répondu au message. Ceux-ci étant le plus à même à se faire abuser à nouveau.
Cyberattaque des ordiphones	Cela commence par un SMS commercial invitant la victime à procéder à une mise à jour payante d'une application. Les pirates informatiques utilisent les coordonnées bancaires immédiatement après que l'utilisateur a saisi l'information.

ID n° 10 attaques humaines

➔ *LES ATTAQUES ORGANISATIONNELLES*

L'utilisation des failles d'une organisation, permet d'accéder à ses données sensibles.

Les sous-traitants et prestataires représentent une porte d'entrée physique d'une organisation pour y commettre des méfaits. Certains n'hésitent pas à passer à l'action comme nous le mentionnions en utilisant des portes d'entrées logiques.

Statistiquement, les courriels infectés par des ransomwares sont adressés plus particulièrement, entre le mardi et le jeudi. Les chevaux de Troie bancaires, eux sont adressés le mercredi, les campagnes sur les points de vente (PDV) jeudi et vendredi et les keyloggers et back Doors sont envoyés le lundi.[117]

TYPE D'ATTAQUE	EXPLICATION
Menaces persistantes avancées	Les Menaces persistantes avancées (APT) sont des opérations d'espionnage industriel (vol de secrets commerciaux ou propriétés intellectuelles) ou dans le but de détruire ou compromettre des plans et infrastructure d'une entreprise. Les pirates utilisent des techniques basées sur la messagerie pour lancer leur attaque. Ils procèdent comme le vol d'information par des agences de l'état, pour récolter des données et accéder au système. Leur tactique est de s'introduire sans se faire remarquer des organisations, en dehors des heures de bureau et laisser des portes dérobées au cas ils seraient repérés pour réitérer leur attaque. C'est pourquoi ces attaques sont nommées « persistantes ». Ces professionnels utilisent toutes les techniques de piratages à leur disposition et ont le savoir-faire pour développer, eux-mêmes leurs propres outils pour s'adapter à leur environnement.
Attaque des terminaux ou « Endpoint-Delivered Threats »	Les pirates se reposent sur les terminaux utilisés dans l'organisation pour s'introduire dans le système. Leur tactique est : Connecter un appareil infecté au réseau de l'organisation qui propagera un code malveillant Connecter un appareil mobile infecté Utiliser un employé qui va charger un logiciel malveillant comme un faux antivirus ou autre nettoyeur de disque dur. Laisser, innocemment des clefs USB, abandonnée sur une table, un parc de stationnement, en espérant qu'une personne de l'organisation la ramasse et la connecte sur son ordinateur.

ID n° 11 attaques organisationnelles

[117] Proofpoint, édition 2017 du rapport « Le facteur humain »

1.6.2. LES ATTAQUES MARQUANTES

TYPE D'ATTAQUE	EXPLICATION
WannaCry	L'attaque « WannaCry », en mai 2017, est à ce jour inédite, 300 000 victimes ont été répertoriées dans plus de cent cinquante pays (voir Annexe n°13 page 188). Cela démontre la fragilité de la sécurité des organisations. Ce ransomware a coûté un milliard de dollars à l'économie mondiale, a touché 10 à 15 millions d'ordinateurs et 190 pays[118]. De grandes organisations comme les chemins de fer allemands, la principale compagnie de télécommunication espagnole, l'organisation de logistique américaine FedEx et le Ministère de l'intérieur russe ont été impactées. Microsoft a reçu une demande d'aide financière de l'Inde, le sommant d'aider les propriétaires d'ordinateur de ce pays, à remplacer le système d'exploitation XP – non protégé de WannaCry — par Windows 10 119.
Locky	Apparu début 2016, ce ransomware est devenu, en un an, le plus répandu dans une centaine de pays et auprès des organisations, qu'il réussit à bloquer (voir §2.3 page 63) Ce vers se cache dans un document Word, Excel ou PDF et ressemble à s'y méprendre à un reçu de paiement ou de document « officiel ». Cette méthode dite « *miroir* » permet de contourner les antispams[120].
Conficker	Ce ver a exploité une faille de Windows, en 2008. Il a fait 15 millions de victimes (environ).
NotPetya (autrement appelé NotPetya, Petna, ExPetr)	Né en Ukraine, d'après Guillaume Poupard, Directeur de l'ANSSI, son but est de faire le maximum de dégâts dans les entreprises. De grandes entreprises comme Saint Gobain, Maersk (transport maritime) ou encore WPP (publicité) ont été touchées. Pour certaines, 80 % de leur informatique a été stoppée. Le réseau de 12 000 sociétés ukrainiennes a été touché dont le site de la centrale de Tchernobyl, le métro de Kiev, les banques, les groupes multinationaux Nivea, Auchan, Saint Gobain… Le rançongiciel a bloqué la surveillance automatique de la radioactivité de la centrale de Tchernobyl, les ouvriers ont dû procéder aux mesures manuellement, avec les vieux compteurs Geiger.

ID n° 12 attaques marquantes

1.6.3. LA MENACE DES PERIPHERIQUES EXTERNES

La prolifération de périphériques de stockage externes de grande capacité constitue une menace, comme : les clés USB, les lecteurs et graveurs de CD et de DVD amovibles, les ordiphones, les tablettes dotées d'une capacité de stockage de données.

Ces matériels représentent deux grandes catégories de risques :

- L'introduction de codes malveillants sur le réseau,
- La perte ou le vol de données de l'organisation.

---

118 La cyberattaque WannaCry a coûté 1 Md USD à l'économie mondiale https://fr.sputniknews.com/international/201705251031524729-cyberattaque-economie-mondiale/

119 WannaCry pourrait coûter des milliards de dollars à Microsoft http://www.journaldugeek.com/2017/07/04/wannacry-milliards-dollars-microsoft/. Windows XP est le système le plus utilisé en Inde. Un nombre conséquent de licences illégales est installé car, le prix élevé de 110€ pour une version standard, ne permet pas aux possesseurs d'ordinateurs d'opérer une mise à jour.

120 Le spam, courriel indésirable ou pourriel est une communication électronique non sollicitée, en premier lieu via le courrier électronique. Il s'agit en général d'envois en grande quantité effectués à des fins publicitaires. https://fr.wikipedia.org/wiki/Spam

- L'utilisation des matériels professionnels à des fins privées revient sur le devant de la scène, en particulier par les dirigeants des organisations[121], ainsi que le BYOD qui génère des compromissions à partir d'URL frauduleuses.[122]

1.7. QUE PROTEGER ?

1.7.1. LES DONNEES A CARACTERE PERSONNEL

Pourquoi protéger les données à caractère personnel ?

Le fait de protéger les données à caractère personnel de ses clients, de son personnel ou de ses patients, permet de renforcer la sécurité, donc d'être moins exposés vis-à-vis des pirates et également de sanction juridique en cas de divulgation ou compromission.[123]

Les organisations, doivent prendre conscience que, cette attitude renforce leur image, et peut être un avantage par rapport à la concurrence.

La notion de « *données personnelles* » est apparue avec l'informatique, la collecte et le traitement des données, à ne pas confondre avec celle de « *vie privée* », qui existe depuis le XIX siècle. Dès 1970, plusieurs pays ont commencé à réglementer la protection des données personnelles avant que la préoccupation devienne mondiale dans les années 1980.

Toutes les données personnelles ne relèvent pas de la vie privée. Par exemple les données de la vie publique d'une personne sont des données personnelles mais pas de sa vie privée. Le droit à la vie privée est la possibilité de garder une part d'intimité.

➔ *LES DONNEES PERSONNELLES DES PATIENTS*

Les établissements de santé sont de grands générateurs d'informations, collectées principalement, dans le dossier patient informatisé ou papier et dans les logiciels métiers.

Les patients demandent de plus en plus de garanties de sécurité quant à leurs données personnelles. 80 %[124] des personnes indiquent que les données de leur dossier médical sont sensibles et ne souhaitent pas partager celui-ci avec tout organisme en faisant la demande (paradoxal par rapport à la valeur attribuée à leurs données de santé §1.3.3 page 24) et considèrent les établissements de santé comme des zones de confiance (39 %)[125].

---

121 IDC est un acteur majeur de la Recherche, du Conseil et de l'Évènementiel sur les marchés des Technologies de l'Information, et des Télécommunications. http://www.idc.fr/. 71 % des sondés jugent très préoccupante l'utilisation privée d'équipements mobiles, en particulier par les dirigeants.

122 Proofpoint, édition 2017 du rapport « Le facteur humain ». Les compromissions, à partir d'URL frauduleuses, arrivent pour 50% de terminaux ne faisant pas parti du parc maintenu par les organisations. Les clics sur ces URL sont effectués pour 42% à partir de terminaux mobiles.

123 Fabrice Mattatia, *Le droit des données personnelles*, Eyrolles Collection, édition n°2

124 Source https://www.frenchweb.fr/tag/ronan-le-quere

125 « *Crossing the Line* » réalisée par KPMG. Etude réalisée par KPMG a interrogé auprès de 7 000 personnes, originaires de 24 pays, https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2016/11/crossing-the-line.pdf, janvier 2017

Les professionnels de santé, ne prennent pas conscience de la duplicité des pirates et, utilisent des données de leurs patients en dehors de toute sécurité ou, sans en informer leur patient comme le montre l'exemple suivant :

> *Une pédiatre de l'AP-HM, qui a procédé à un traitement automatisé de données médicales, sans l'autorisation de la CNIL a été condamnée à une peine de 5 000 € d'amende, par un jugement définitif du TGI de Marseille du 7 juin 2017* [126].

La réglementation, notamment la mise en place du RGPD le 25 mai 2018, abonde dans ce sens en durcissant les contrôles et appliquant des sanctions financières qui vont de 2 % à 4 % du chiffre d'affaires, ou budget, annuel mondial de l'organisation.

En 2017, 3 442 748 dossiers de santé ont été compromis (13 425 263 signalés en 2016). De grandes institutions de santé ont été visées en 2015[127], comme Anthem (78,8 millions d'enregistrements), Premera Blue Cross (11 millions d'enregistrements) et en 2016, Banner Health (3,6 millions d'enregistrements) et Newkirk Products (3,4 millions d'enregistrements).

Les dossiers médicaux électroniques peuvent être vendus à 50 dollars l'unité sur le marché noir.

Les attaquants ont rodé leur technique et diversifient leurs « clientèles » en se tournant vers de plus petites entités. Ils ont également amorti leur temps de recherche et de développement ou font appellent à des « ransomware prêt à l'usage ». Ils élargissent leurs cibles aux cabinets médicaux, centres chirurgicaux, laboratoires de diagnostic, centres d'IRM et de tomodensitométrie.

Plusieurs exemples de cyberattaques démontrent la vulnérabilité des établissements de santé et l'intérêt des attaquants :

- La London Bridge Plastic Surgery a déclaré avoir été la victime d'une cyberattaque le 17 octobre 2017. D'après The Daily Beast[128], le groupe *The Dark Overlord* a revendiqué la cyberattaque et a assuré avoir en sa possession des téraoctets de données qu'il a menacé de publier, dont certaines touchant « des familles royales. ».
- Autre exemple : Un groupe de pirates, nommé Pravvy Sector, a mis en ligne 150 Go de données médicales d'un réseau de cliniques d'urologie de l'Ohio en mai 2016[129].
- L'organisation Health South-East RHF a été victime d'une attaque le 8 janvier 2018. Cette agence gère les hôpitaux du sud-est de la Norvège, qui est la plus grande région sanitaire avec des établissements de santé qui traite 2,9 millions de personnes sur un total de 5,2 millions d'habitants.[130]

Cette tendance augmentera très sensiblement cette année et en 2019.

---

126 Source https://www.editions-legislatives.fr/actualite/donnees-de-sante-un-medecin-condamne-pour-mise-en-oeuvre-d-un-traitement-sans-autorisation

127 Help Net Security

128 Article paru dans The daily beast, « Hackers Steal Photos From Plastic Surgeon to the Stars, Claim Trove Includes Royals », https://www.thedailybeast.com/hackers-steal-photos-from-plastic-surgeon-to-the-stars-claim-they-include-royals, 23/10/2017

129 Article paru dans Motherboard : https://motherboard.vice.com/en_us/article/bmvd3v/hacker-dumps-sensitive-patient-data-from-ohio-urology-clinics, 02/08/2016

130 Helsedirektoratet.no, https://helsedirektoratet.no/nyheter/innbrudd-i-datasystemene-i-helse-sor-ost, 15/01/2018

➔ *TRAITEMENT DES DONNEES PRIVEES AUX ETATS UNIS*

Les états Unis ont promulgué une loi, fin mars 2017, supprimant la protection de la vie privée de leurs concitoyens. Des Fournisseurs d'Accès Internet (FAI) comme Comcast[131], ATT [132] peuvent revendre, les données à des annonceurs, par exemple, ou les exploiter eux-mêmes à des fins mercantiles.

➔ *LES FAI (FOURNISSEURS D'ACCES A INTERNET)*

Orange, un des premiers l'opérateur téléphonique français a avoué avoir le mardi 6 mai 2014, avoir été victime d'un nouveau vol de données personnelles concernant 1,3 million de ses clients et prospects. Orange avait déjà été attaqué trois mois auparavant et ou 800 000 comptes étaient concernés.[133]

L'ANSSI, a compris que l'on pouvait enrayer la prolifération massive des attaques, en travaillant directement avec les fournisseurs d'internet.

Les FAI et hébergeurs sont déclarés comme « systèmes d'information d'importance vitale ». L'ANSSI compte sur les opérateurs pour détecter à la source les attaques avant qu'elles n'arrivent chez leur client. L'ANSSI, fournira les IOC (indicateur de compromission) aux opérateurs qui auront installé les outils de détection sur leur réseau. Cette disposition est prévue à l'article 19 de la future loi de programmation militaire pour la période 2019-2025.

➔ *LES DONNEES PERSONNELLES SUR LES RESEAUX SOCIAUX*

L'usage gratuit d'un outil cache souvent une exploitation financière à l'insu de l'utilisateur ou pas.

En échange de la collecte des données personnelles, il est concédé un usage gracieux des services. Les données, ainsi récoltées, sont valorisées et mise sur le marché, sans que leurs propriétaires, originels, en touchent le moindre bénéfice.

Les données peuvent être catégorisées en quatre domaines :

- Les données publiques : date de naissance, coordonnées, profession, organisation où l'on travaille, centre d'intérêt, liens familiaux, etc.
- Les informations sécurisées par les paramètres de confidentialité du réseau social : publications accessibles uniquement par les relations de l'utilisateur, les messages privés, les discussions dans les tchats,
- Les informations générées par d'autres consommateurs du réseau et liées à une personne.
- Les données générées par le réseau social, lui-même, en fonction des usages de l'utilisateur. Il s'agit de datamining.

Facebook est le réseau social le plus utilisé au monde. Selon la firme, 350 millions de photos sont déposées sur le site chaque jour dans le monde. Récemment, Facebook a dû modifier sa politique de conservation des données, en proposant « un vrai » droit à l'oubli à ses clients, malgré tout,

---

131 Comcast Corporation est un groupe de médias américain dont le siège est situé à Philadelphie, en Pennsylvanie.

132 AT&T est le plus grand fournisseur de services téléphoniques locaux et longues distances des États-Unis et le 2e opérateur de services mobile. Le siège social mondial d'AT&T est basé à Dallas, au Texas.

133 Source www.scoop.it

cette entreprise est décriée sur l'exploitation qu'elle peut faire des données personnelles.

Une étude de l'université de Louvain, en Belgique, démontre que Facebook viole, la réglementation en matière de vie privée et plus précisément pour le non-respect de la nouvelle loi européenne adopté en janvier 2016[134]. La cour d'appel de Bruxelles, en 2016, à conforter Facebook dans ses agissements au sujet d'un cookie utilisé pour suivre les internautes, non-membres, de son réseau [135].

L'association *Europe-v-Facebook*[136] fait remarquer, également, que Facebook ne respecte pas la réglementation européenne et de surcroît participe au programme *Prism*[137] de la NSA[138]. En France, Facebook[139] a été condamné à une amende de 150 000 euros par l'autorité française de régulation des données (CNIL), pour des manquements à la loi informatique et libertés en mai 2017.

« La vie privée est devenue un enjeu collectif », selon le sociologue Antonio Casilli[140],

Un jeu de « cache-cache » est permanent entre les pouvoirs publics, les internautes et les GAFAM (Google, Apple, Facebook, Amazon, Microsoft) ; ou les chinois BATX pour Baidu, Alibaba, Tencent et Xiaomi ; ou bien les Natu (Netflix, Airbnb, Tesla, Uber).[141].

1.7.2. LES MATERIELS, OBJETS PHYSIQUES

➔ *QUE FAIRE DES MATERIELS EN FIN DE VIE ?*

Souvent, le service informatique, pense que les ordinateurs, retirés du parc et stockés dans un entrepôt sont sans danger ! C'est faux !

Que deviennent les informations, que tout utilisateur, enregistre sur le disque dur de son ordinateur ? Surtout si celui-ci est issu d'un secteur d'activité sensible comme la santé, le nucléaire, etc.

Bon nombre d'entreprises se débarrassent de ses vieux matériels auprès de courtiers en

---

134 Article paru dans Le Parisien.fr, « Vie privée : Facebook épinglé pour non-respect des règles européennes », février 2015

135 Le cookie est l'équivalent d'un fichier texte de petite taille, stocké sur le terminal de l'internaute. Les cookies ont toujours été plus ou moins controversés car contenant des informations personnelles résiduelles pouvant potentiellement être exploitées par des tiers.

136 Max Schrems étudiant en droit autrichien, est à la tête d'un groupe privé, Europe v Facebook. Article paru dans Sophos, 21/06/2014

137 PRISM, également appelé US-984XN1, est un programme américain de surveillance électronique par la collecte de renseignements à partir d'Internet et d'autres fournisseurs de services électroniques. Ce programme classé, relevant de la National Security Agency (NSA), prévoit le ciblage de personnes vivant hors des États-Unis. Edward Snowden, ex-consultant de la NSA, a dénoncé ce programme en 2013.

138 Article paru dans Sud-Ouest « Qui est Max Schrems, ce juriste qui porte plainte contre Facebook ? », 8 août 2014

139 Source les Echos : https://www.lesechos.fr/tech-medias/hightech/0212094723912-donnees-personnelles-facebook-condamne-2087308.php

140 Antonio Casilli, est un sociologue spécialiste des réseaux sociaux. Il est maître de conférences en humanités numériques à Télécom ParisTech et chercheur au Centre Edgar-Morin de l'EHESS

141 Casilli, Antonio A. « Contre l'hypothèse de la fin de la vie privée ». La négociation de la privacy dans les médias sociaux." Revue française des sciences de l'information et de la communication 3 (2013)

informatique, les donnent à des associations ou l'envoient à l'étranger dans des écoles, sans se soucier de ce qu'il pourrait rester sur ces machines.

Des procédures de mise au rebut du matériel seront rédigées et respectées impérativement par les techniciens informatiques.

➔ *ET ENCORE*

TOUT matériel qui est relié à internet est sensible

Voici quelques exemples, surprenants [142], à prendre en compte, même si certains, font sourire… jaune :

- La société Context à mise à jour une faille de sécurité de l'ampoule Lifx Wi-Fi[143]. Ils ont étudié le microcontrôleur de l'ampoule pour comprendre le mécanisme de cryptage, se sont introduits dans le réseau, ont récupéré et décrypté les informations de configuration du réseau. L'équipe a également trouvé des failles dans des imprimantes.
- En août 2013, un pirate informatique a pris le contrôle de la caméra de surveillance (de marque Foscam), installé dans la chambre d'un bébé, dans l'Ohio aux états Unis. Les parents ont entendu des voix provenant de la chambre de leur enfant. Des pirates ont piraté des ours en peluche en Californie, deux millions de conversations ont été piratées et mises en lignes sur internet[144].
- Un groupe de pirates a pris possession de frigo connecté, en Californie en janvier 2014. Les pirates utilisaient les matériels pour envoyer des pourriels. Ils avaient également piraté des ordinateurs, des smart TV[145] et du média center[146].
- Plus proches de nous les objets connectés tel que les assistants personnels intelligents Alexa (Amazon), Google Home (Google), Siri (Apple), Bixby (Samsung), Cortana (Microsoft) sont piratables. Des chercheurs de l'université du Zhejiang, en Chine ont transmis des commandes vocales à des fins malveillantes, à ces dispositifs, à l'insu du propriétaire. L'attaque se nomme *DolphinAttack*, il suffit d'envoyer des commandes vocales ultrasoniques, situées entre 20 kHz et 10 MHz aux systèmes de reconnaissance vocale. Ces sons sont inaudibles pour l'être humain. Les chercheurs ont réussi, entre autres, à activer Siri pour lancer un appel Face Time sur un IPhone et manipuler le système de navigation d'une voiture de la marque Audi.[147]
- Les jouets connectés comme le robot *I-Que* et la poupée *My Friend Cayla*,[148] comporte de graves failles de sécurité. Les agents de la CNIL, ont effectué des tests de piratage, positionnés à 20 mètres du jouet. Ceux-ci ont pris le contrôle de ces petites machines, ont entendu et enregistré toutes les paroles échangées entre l'enfant et le jouet ou les conversations se déroulant à proximité.

---

142 « Loterie IoT: trouver un appareil connecté parfaitement sécurisé » https://securelist.com/iot-lottery/83300/, 27/11/2017

143 Lifx est une ampoule intelligente que vous pouvez contrôler avec votre smartphone.

144 https://mashable.com/2017/02/27/internet-of-things-cloudpets-hacking/#_q3gGjr8JSq9

145 Téléviseur connecté ou intelligente (smart)

146 Centre multimédia est un matériel qui permet de lire des fichiers multimédias (image, son et vidéo)

147 Etude DolphinAttack: Inaudible Voice Commands, https://endchan.xyz/.media/50cf379143925a3926298f881d3c19ab-applicationpdf.pdf

148 Mise en garde de la CNIL https://www.cnil.fr/fr/jouets-connectes-mise-en-demeure-publique-pour-atteinte-grave-la-vie-privee-en-raison-dun-defaut-de, 04/12/2017

Le piratage est dans les outils de la vie quotidienne, les utilisateurs peuvent se retrouver démunis ou ignorants face à ces dangers, les industriels doivent renforcer la sécurité.

➔ *QU'EN EST-IL DES OBJETS CONNECTES EN SANTE ?*

Les IOT sont de plus en plus utilisés dans le domaine médical ; c'est un domaine dynamique qui se développe en France. Ce marché est évalué à 4 milliards d'euros pour la France d'ici 2020. Les éditeurs et autres constructeurs ont investi près de 100 millions d'euros[149] dans la e-santé en 2016.

Les usages sont multiples comme [150] :

- Ochsner Health System, basé à La Nouvelle-Orléans, intègre son dossier de santé électronique (DSE) à l'Apple Watch pour permettre une analyse précise et en temps réel de l'état de santé du patient.
- Surveiller le rythme cardiaque avec l'Apple Watch,
- La détection et l'apparition d'un AVC avec le *CardioNexion* avec leur tee-shirt connecté,
- Les vêtements de la société *Bioserenity* pour surveiller les personnes épileptiques,
- Les montres connectées de la société Pkvitality pour surveiller le taux de glycémie.

Ces outils de surveillances, sont au plus près de l'intimité de leurs utilisateurs.

Les fabricants veulent avant tout vendre leur produit, et parfois font l'impasse sur la sécurité, et aussi par manque de connaissance de l'ingéniosité des pirates informatiques.

1.8. COMMENT SE PROTEGER OU ANTICIPER

1.8.1. ANTICIPER LES ATTAQUES POUR PREVENIR

La veille sécurité est indispensable, le RSSI et le DSI s'informeront sur les dernières technologies du marché, comme la blockchain, l'Intelligence Artificielle qui pourrait apporter des solutions de sécurité.

➔ *LE SOC (SECURITY OPERATING CENTER) OU « CENTRE D'OPERATIONS DE SECURITE RESEAU »*

Les SOC sont encore rares dans les entreprises françaises, car leur mise en œuvre représente un coût élevé. On pourrait comparer cette organisation à un SOC dans le bâtiment qui est constitué d'agents de sécurité qui vérifient les accès au bâtiment, les lumières, les alarmes, les barrières de véhicules, etc.

Cette organisation est liée aux personnes, aux processus et aux technologies déployées dans l'organisation et permet, par la collecte d'informations de s'assurer qu'il n'existe pas de menace informatique en cours. Généralement, cette plateforme analyse des évènements sous forme de logs envoyés par les équipements de sécurité (pare-feu, IDS/IPS, VPN, antivirus, etc.), ou réseau. Des processus de gestion des incidents sont appliqués afin de s'assurer que les incidents détectés sont signalés, analysés et traités.

Les applications sont également mises sous surveillance afin de détecter toutes attaques

---

149 Sources www.journalducm.com

150 « 16 startups françaises qui dessinent le futur de notre santé » https://www.maddyness.com/innovation/2017/09/05/ia-16-startups-francaises-futur-sante/, 19/09/2017

(cyberattaques, virus, etc.) et des outils d'analyse comportementale sur les postes sont également installés. Le croisement des informations, remontées en temps réel permet de mettre au jour des anomalies, dont les intrusions.

Les outils de surveillance évoluent, ainsi que la réglementation qui durci les contrôles en matière de traçabilité (génération de logs dans les applications, par exemple).

Le SOC permet de minimiser les risques et d'être plus réactifs aux menaces, donc de mieux protéger l'organisation et ses informations. On pourrait qualifier le SOC de « Tour de contrôle de la protection de l'information ».

➔ *SUIVI EN TEMPS REEL DES ATTAQUES*

Des éditeurs d'antivirus ou constructeurs, mettent à disposition des cartes de surveillance des attaques se produisant en temps réel. Ces cartes peuvent être intéressantes à consulter afin de s'informer des attaques en cours sur la planète.

Certaines sont axées sur des outils attaqués, comme la messagerie ou des solutions comme le SaaS, et, sont souvent promues par les éditeurs de solution de sécurité ou des sociétés de cyber sécurité (voir Annexe n°20 page 209).

➔ *LES CERT (COMPUTER EMERGENCY RESPONSE TEAM)*

Un CERT (ou CISRT, Computer Security Incident Response Team), est une organisation gouvernementale ou d'une organisation privée. Elle a pour mission de gérer, traiter les alertes à la suite d'incidents et de prévenir des incidents de sécurité. Il réagit et proagit en collectant des données de sources externes à l'organisation, dont les alertes seront traitées avec des analystes.

Il est souvent possible de s'abonner au flux RSS de ces CERT, afin de recevoir les alertes en direct (voir Annexe n°21 page 210).

➔ *LES BLOGS DE SECURITE*

Krebs on security https://krebsonsecurity.com/	Fortinet https://blog.fortinet.com/archive
Sophos https://nakedsecurity.sophos.com/	FSecure https://business.f-secure.com/
Kaspersky https://securelist.com/	Microsoft https://blogs.technet.microsoft.com/msrc/
Debian http://security.debian.org/	Sans Incident Handlers Diary https://isc.sans.edu/
Blog de Sécurité d'Oracle http://blogs.oracle.com/	

➔ *LES PASSERELLES DE SURVEILLANCES MULTIPLES*

- Vigilance (https://vigilance.fr/).
- Le CERT-XMCO est un CSIRT commercial français, (http://www.xmco.fr/veille-vulnerabilite-securite-cert-xmco-fr.html)

1.8.2. LES MOYENS DE PROTECTION ET DETECTION A METTRE EN PLACE

Le bon sens dictera la conduite de la DSI et du RSSI En matière de sécurisation de l'information.

Les moyens mis en œuvre doivent, répondre aux besoins de sécurisation, tout en permettant aux employés de travailler dans de bonne condition.

L'ANSSI a édité un guide des solutions certifiées par leurs soins, pour sécuriser le réseau, les ordinateurs, ainsi que les sociétés prestataires de services de sécurité.

Il est recommandé de faire appel à ces solutions et sociétés, et éviter les écueils d'une société qui vend du rêve après être passée proche du cauchemar. C'est-à-dire, adresser un rapport d'audit « *hypercatastrophique* », ne reflétant pas toujours la réalité, mais surtout proposant un nombre incalculable d'heures de prestation pour remettre le système d'information sur les rails de la sécurité.

Les outils les plus courants pour se protéger sont :

- Un antivirus sur toutes les machines (ordinateurs et serveurs), fonctionnel et à jour.
- Un pare-feu. Ce dispositif analyse tous les flux entrants, sortant et vérifie les ports que l'on a autorisés. Cela permet de protéger un ordinateur ou un réseau des ingérences d'un réseau comme internet,
- Un proxy et reverse proxy[151], qui filtrera toutes les adresses URL que vous autorisez ou non,
- Un anti spam, qui filtrera les messages indésirables,
- L'usage des VPN (Virtual Private Network), réseau virtuel privé. Il s'agit d'un tunnel privé entre un point de départ et un point d'arrivée. Il peut être utilisé pour les prestataires, qui se connectent au réseau de l'entreprise, pour se connecter à la messagerie ou l'extranet de l'entreprise…
- Il est également, indispensable de compartimenter le réseau de l'entreprise, pour perdre l'attaquant ou le ralentir. Il est d'usage de séparer le réseau par usage métier ou criticité des applications stockées sur les serveurs. Ce système se nomme VLAN[152].
- Une zone tampon ou DMZ[153] (DeMilitarized Zone), entre le réseau de l'entreprise et l'extérieur est mise en œuvre pour héberger les applications dont on peut accéder de l'extérieur (site internet hébergé en interne, extranet, messagerie, FTP public, etc.).
- Des outils d'analyse comportementale sur les postes et serveurs, afin de détecter une augmentation de flux, par exemple, en cas d'usage d'un poste dans un réseau de Bot (ensemble de machines zombies piratées).

L'ensemble de ces outils seront complétés par une politique de sécurité et la sensibilisation des utilisateurs.

Les outils mis en place limiteront juste les dégâts lorsqu'un employé cliquera sur le lien dans le faux message ou ouvrira la pièce jointe.

1.8.3. LES MOYENS DE PROTECTIONS MIS EN PLACE

Le CLUSIF [154] réalise une enquête tous les deux ans, auprès des acteurs publics et privés de tous secteurs économiques, sur la « *Menaces informatiques et pratiques de sécurité en France* ». L'étude est basée sur la norme ISO 27002 (les bonnes pratiques en matière de sécurité des systèmes d'information).

Un domaine public, différent, est étudié tous les deux ans, les établissements de santé ont répondu

---

151 Un reverse proxy est un type de serveur, habituellement placé en frontal de serveurs web. Contrairement au serveur proxy qui permet à un utilisateur d'accéder au réseau Internet, le reverse proxy permet à un utilisateur d'Internet d'accéder à des serveurs internes, une des applications courantes du reverse proxy est la répartition de charge.

152 Un VLAN (Virtual Local Area Network ou Virtual LAN, en français Réseau Local Virtuel) est un réseau local regroupant un ensemble de machines de façon logique et non physique.

153 http://www.commentcamarche.com/contents/991-dmz-zone-demilitarisee

154 Club de la Sécurité de l'Information Français

à l'enquête en 2018.

Le CLUSIF a questionné 350 entreprises de plus de 100 salariés (Banque Assurances, Commerce, Industrie BTP, Services, Transport – Télécoms) et 250 établissements de santé.

Le RSSI a été particulièrement visé dans le cadre de cette enquête où il a répondu pour 25 % des cas et à 40 % pour les entreprises de plus de 2000 salariés. Les autres répondants, à 73 % sont les DSI, les Directeurs ou Responsables informatiques.

Les particuliers ont été également sondés (1 000 personnes) afin de comprendre l'évolution de leur vision d'internet et de ses usages.

Le budget consacré à la sécurisation de l'information est stable et est, essentiellement tourné vers la mise en place de solutions techniques (23 %). La prise en compte organisationnelle est difficile et nuit à la maturité de la sécurité dans les organisations.

Les établissements de santé, s'organisent en GHT (Groupement Hospitalier de Territoire) et montent en maturité. Ils sont, en majorité (81 %) incapables d'évaluer les coûts de la sécurité et réalisent, pour un tiers seulement, une analyse d'impact des coûts financiers sur les incidents. Ceux-ci sont « poussés » par le ministère de la santé à sécuriser le système d'information hospitalier avec la clef des subventions (hôpital numérique, plan sécurisation 2018, etc.). Les dossiers sont instruits, si certains prérequis, dont des bases de la sécurité, sont mis en place (PSSI, gestion d'accès sécurisé des applications de santé, etc.). L'ARS (Agence Régional de Santé) a également exigé un plan d'action sur 2 ans.

La certification de l'HAS (Haute Autorité en Santé) propose, depuis la version 2014, une vision « PDCA », en adéquation avec la démarche de sécurisation et plus seulement sur la présentation de la preuve. La Direction qualité accompagne les responsables de la protection de l'information. Elles les forment, souvent, à l'analyse de risques, à leur cotation et à la mise en place d'un plan d'action. Ce dernier est exigé et, vérifié régulièrement par les experts visiteurs par l'intermédiaire d'une plateforme SARA.

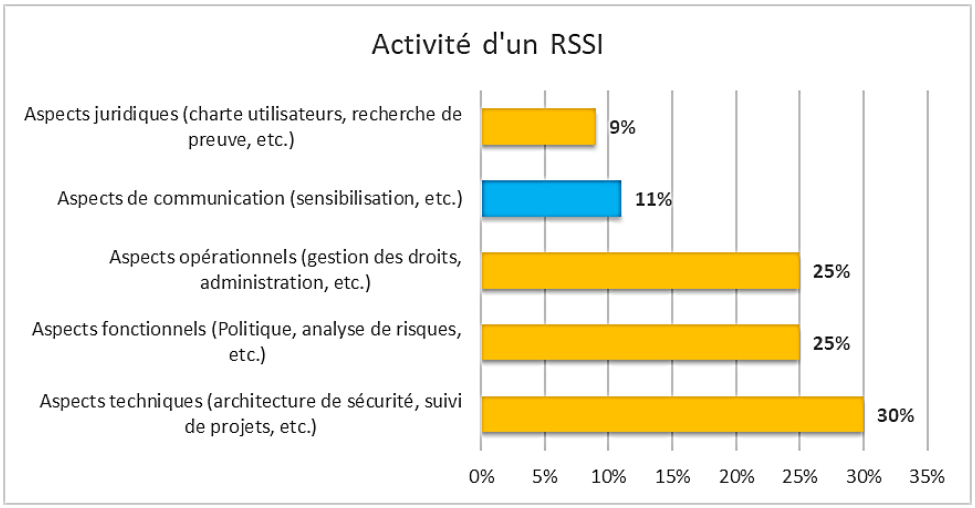
L'encadrement de la sécurité, par la mise en place d'une politique de sécurité est en augmentation, dans le privé et le publique, exception des organisations de moins de 200 salariés. La DSI est rédactrice de cette charte à 73 % alors que ce rôle, reviendrait logiquement au RSSI. Ce document est maintenu et diffusé auprès des acteurs de l'organisation.

Les établissements de santé font état d'un manque de budget et de compétences. Le métier de RSSI, était souvent occupé à mi-temps ou moins, soit par le DSI ou le Responsable réseau / système. Ce métier se professionnalise et est occupé à temps plein.

L'origine du RSSI explique, peut-être, la prédilection des aspects techniques de la sécurité. Le RSSI est souvent la même personne qui a abandonné une partie de son activité pour se consacrer à plein temps à la mission de la protection de l'information.

Des actions de sensibilisation sont mises en place dans 50 % des cas et seulement mesurées pour 15 % des organisations.

Le RSSI se consacre aux tâches suivantes dans son organisation :



ID n° 13 Activité du RSSI dans son organisation

La sensibilisation arrive en avant dernière position, a contrario des aspects techniques qui occupent le RSSI le plus clair de son temps. Le renforcement de la sécurité physique des outils de travail (ordinateur, ordiphone, tablette) est généralisé (pare-feu sur les ordinateurs portables, antivirus sur les appareils mobiles).

L'expérience de WannaCry and Co a renforcé le suivi du déploiement des patchs de correction et la veille sécurité sur les vulnérabilités des systèmes de l'organisation.

L'usage des appareils personnels (BYOD) est interdit majoritairement (72 % dans le privé et 77 % dans le public) dans les organisations interrogées. On peut s'interroger sur la considération des acteurs de l'organisation par les responsables de la sécurité. Les acteurs sont soumis à des interdictions, des contraintes et ne sont pas sensibilisés – ou peu —.

Une PSSI est-elle suffisante pour sensibiliser les acteurs de l'organisation ?

Les chiffres remontés lors de cette enquête parlent d'eux-mêmes : les organisations ont subi des infections virales (44 %) avec des pertes de services essentiels (22 %). Elles ont été la cible de phishing (64 %) et de fraude au président (17 %).

Les outils de sécurité techniques sont-ils suffisants pour protéger l'organisation ?

Malgré ce constat, seulement 41 % des organisations ont mis en place une cellule d'analyse des incidents et se sont posé les bonnes questions : les hommes et femmes qui constituent la force de notre organisation peuvent-ils (elles) nous aider à combattre la cybercriminalité, au quotidien devant leur ordinateur ?

Des audits techniques sont menés tous les deux ans environ (66 % dans le privé) et une à cinq fois par an pour les établissements de santé.

Ces audits sont exigés par des besoins réglementaires ou par l'assureur de l'organisation. Les audits organisationnels n'ont pas l'intérêt des organisations, aucune information n'est indiquée sur ce sujet, ce qui corrobore les chiffres annoncés plus haut.

Le protecteur de l'information, le RSSI, est de plus en plus proche de la Direction générale, par son rattachement hiérarchique, ce qui lui donne de la légitimité (49 %), cependant 30 % restent sous l'autorité de la DSI. Cette organisation peut provoquer des conflits d'intérêts.

Les indicateurs de suivi de la protection de l'information sont de moins en moins consignés dans un tableau de bord. On se demande comment sont remontées les informations auprès de la Direction, sur quelles bases sont discutés les budgets, si aucune mesure ne fait apparaître les actions et résultats de celles-ci !

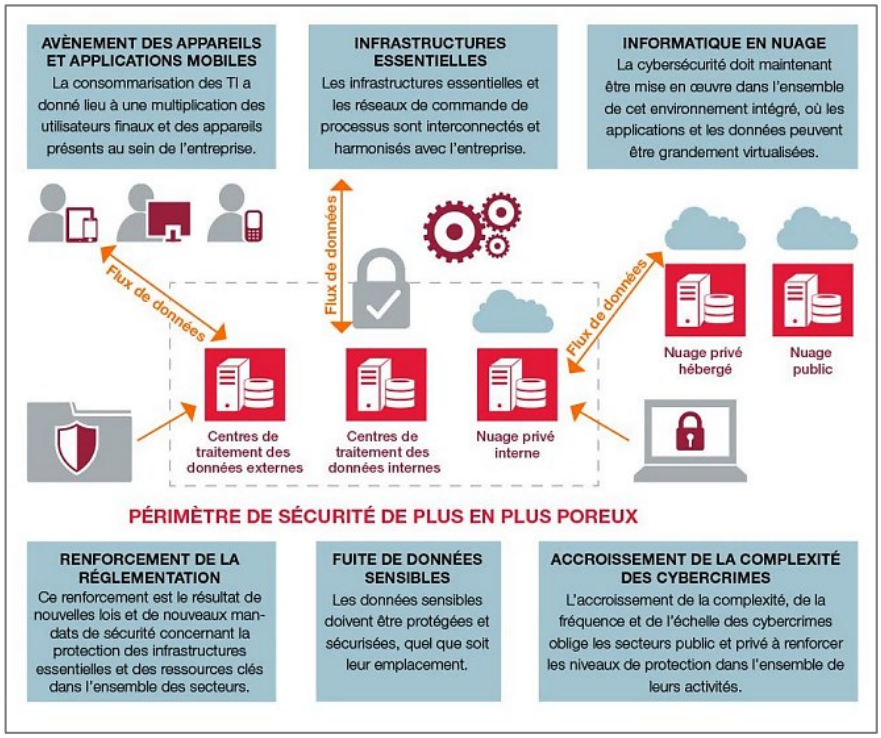
Selon une enquête effectuée en 2016 par la HIMSS (Healthcare Information and Management Systems Society) sur la cyber sécurité, les établissements de santé ont mis en œuvre les outils suivants :

- 86 % ont installé des outils contre les programmes malveillants,
- 81 % utilisent des pare-feu,
- 64 % chiffrent les données en cours de transfert et 59 % chiffrent les données stockées,
- 57 % s'occupent de la gestion des correctifs et des vulnérabilités,
- 52 % ont installé un outil de gestion des appareils mobiles,
- 41 % utilisent une passerelle de sécurité Web et 37 % une passerelle de sécurité pour leur messagerie.

1.9. CONCLUSION

La protection de l'information s'abordera d'un point de vue global.

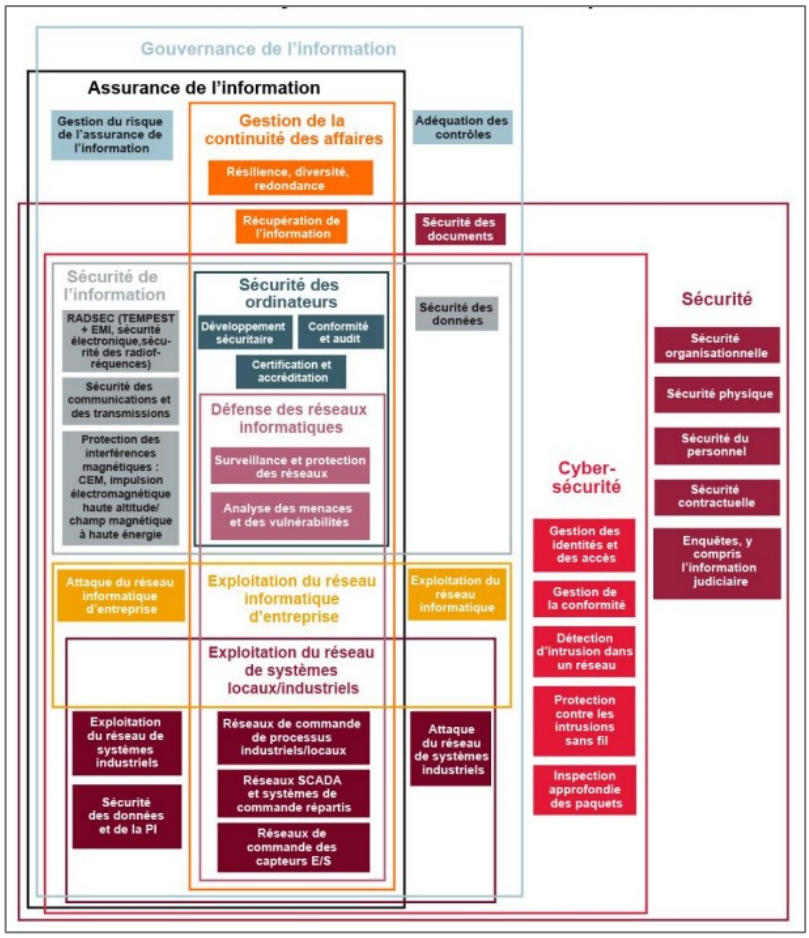
Les univers sont de plus en plus poreux, les données circulent entre les écosystèmes, comme le montre le schéma ci-dessous :



ID n° 14 La cyber sécurité des infrastructures – source CGI 2014

La protection de l'information est essentielle car elle représente le capital immatériel d'une organisation (exemple de l'affaire Wikileaks[155]). Cette protection s'appuiera sur des moyens techniques et surtout sur la formation/sensibilisation des utilisateurs.

La mise en place d'un programme de protection de l'information, intégrera les autres domaines de sécurisation de l'organisation, la complétera, la renforcera et ira de concert dans une grille de lecture globale :



ID n° 15 intégration des autres domaines de sécurisation de l'organisation

L'ouverture des systèmes d'information sur le monde, via internet a créé un « *nouveau paradigme* » auquel une adaptation, par tous les moyens, est nécessaire pour protéger l'information.

[155] Source https://www.lesechos.fr/04/10/2016/lesechos.fr/021135667754 1_les-dix-plus-grosses-revelations-de-wikileaks.htm

CHAPITRE 2
ETAT DE L'ART DE LA PROTECTION DE L'INFORMATION

« Rien n'est permanent sauf le changement »
Héraclite[156]

[156] Philosophe Grec de la fin du VIe siècle av. Jésus Christ.

2.1. INTRODUCTION

Après une revue des risques et des menaces, nous allons regarder le monde de l'information, analyser le retour d'expérience de professionnels de la protection de l'information et les résultats de l'enquête effectuée, entre juillet et novembre 2017 auprès des acteurs de l'organisation.

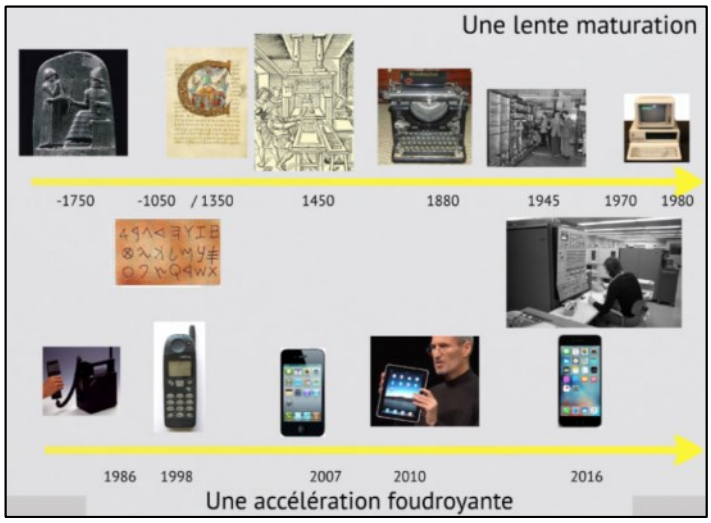
2.2. HISTOIRE DE L'INFORMATION ET INTERNET

L'histoire de l'information remonte à la nuit des temps, depuis que les hommes ont eu une conscience et ont su transmettre des données sur les supports de l'époque.

Le mot Information signifie « *se former une idée de* ». Cette *idée* se forge par la lecture ou la transmission orale. Le moyen de transmission courant est l'écriture.

Les premiers signes de communication sont apparus dans des grottes, avec les peintures rupestres, dessinés par des hommes qui ne se doutaient pas que leurs descendants les admireraient partout dans le monde, via internet.

Le développement de l'écriture est probablement dû à des aspects pragmatiques, comme la comptabilité, l'échange d'information et de connaissance, la diffusion des lois, la mémorisation de coutumes, etc.…



ID n° 16 évolution de l'histoire de l'information

Le support de l'information a évolué, au fil du temps : des tablettes en argile, (Mésopotamie -3 500 ans avant Jésus Christ), en passant par le papyrus (Egypte, -3 000 ans avant Jésus Christ) et le parchemin. Celui-ci sera plus accessible que le papyrus et perdurera jusqu'à la renaissance.

Le papier, invention asiatique et l'arrivée de l'imprimerie avec Gutenberg en 1450, fera la joie des lettrés, car l'information va se diffuser à travers l'Europe.

L'accélération jusqu'à internet va s'intensifier à partir du XIXe siècle. L'information va pouvoir être diffusée plus rapidement entre la « *production* » et la « *consommation* ». La rotative, le train, les ondes hertziennes, les satellites et enfin internet mettent l'information à portée de clic.

Les technologies de l'information sont rentrées dans la vie privée à partir de 1975, avec l'arrivée de la téléinformatique, le Minitel, Internet, les microprocesseurs, les ordinateurs personnels (1980), etc.

D'autres inventions ont contribué à l'accès à internet et au partage de masse de l'information :

- 1978 : Protocole Internet IP (communication par paquet) est mis au point par Lawrence Roberts et son équipe. Ce modèle permet d'emprunter plusieurs chemins de communication.
- 1985 : les adresses URL apparaissent. Paul Mokapetris met au point un système qui permet aux ordinateurs de se retrouver sans système central.
- 1982 : TCP/IP[157] est inventé pour pouvoir utiliser d'autres réseaux moins fiables qu'ARPANET. Vinton Cerf et Robert Khan permettent de vérifier si les paquets sont bien arrivés à destination.
- 1993 : Le premier navigateur internet *Mosaïc* (qui deviendra Netscape) a inventé le format HTML et les liens hypertextes. C'est un pas décisif qui permet à tout un chacun d'accéder à Interner. Le *WWW* (World Wide Web) était né.

Au tout début d'internet, l'accès était réservé à des initiés sachant utiliser du code pour accéder aux informations.

La première page web est bien peu attrayante, par rapport aux sites internet que nous connaissons aujourd'hui. Elle a été mise en ligne le 13 novembre 1990, l'adresse originale était *nxoc01.cern.ch/hypertext/WWW/TheProject.html*.

World Wide Web

The WorldWideWeb (W3) is a wide-area hypermedia information retrieval initiative aiming to give universal access to a large universe of documents.

Everything there is online about W3 is linked directly or indirectly to this document, including an executive summary of the project, Mailing lists , Policy , November's W3 news , Frequently Asked Questions .

What's out there?
Pointers to the world's online information, subjects , W3 servers, etc.
Help
on the browser you are using
Software Products
A list of W3 project components and their current state. (e.g. Line Mode ,X11 Viola , NeXTStep , Servers , Tools , Mail robot , Library)
Technical
Details of protocols, formats, program internals etc
Bibliography
Paper documentation on W3 and references.
People
A list of some people involved in the project.
History
A summary of the history of the project.
How can I help ?
If you would like to support the web..
Getting code
Getting the code by anonymous FTP , etc.

ID n° 17 La première page internet mise en ligne le 13 novembre 1990.

La miniaturisation des supports, couplés avec les moyens télécoms, a permis de transporter l'information jusqu'à nous, dans notre poche. Les outils comme les ordiphones (IPhone en 2007) et tablettes (iPad en 2010) ont révolutionné l'accès au net.

Steve Jobs a changé le paradigme de l'utilisation d'internet, en rendant son usage « *agréable* » à partir de ses outils et a forcé ainsi, les opérateurs à proposer des abonnements avec un accès

[157] TCP (Transmission Control Protocol) et IP (Internet Protocol)

illimité à internet, pour poursuivre sa démarche commerciale.

Les Français ont été précurseurs en matière de communication électronique : ils ont inventé le Minitel en 1980. Le Minitel (*Médium Interactif par Numérisation d'Information Téléphonique*) est un « terminal informatique destiné à la connexion au service français de Vidéotex baptisé Télétel [158] », commercialement exploité en France entre 1980 et 2012

➔ LES IOT (INTERNET OF THINGS OU L'INTERNET DES OBJETS)

Nous abordons une nouvelle révolution de l'internet et du traitement des informations avec les IOT et les nouveaux usages qu'ils vont entraîner.

Un grand nombre d'objets sont connectés à internet : montres, ampoules, caméras de surveillance, téléviseurs, thermostats, voitures, balances, vêtements,… Ce qui engendre, des risques d'intrusion de la part de personnes malveillantes.

Les conséquences d'attaque pourraient être graves si, ces personnes se révèlent être des terroristes ou d'autres états et décident de s'attaquer aux secteurs du transport, de la santé ou de l'énergie.

« *Ils sont censés rendre nos entreprises plus productives et nos existences plus simples, plus saines et plus intelligentes, mais il y a souvent une contrepartie* », observe le Professeur Edward Humphreys, animateur du groupe de travail de l'ISO/IEC sur les systèmes de management de la sécurité de l'information.

> « Nous voulons croire en ces technologies en raison du champ des possibilités qu'elles offrent. Mais nous devons avoir conscience de leurs répercussions sur la sécurité et la confidentialité de nos données. »
> Professeur Edward Humphreys[159]

Malheureusement, la sécurité n'est pas considérée à sa juste mesure, par les constructeurs.

L'usage des IOT aura presque doublé en cinq ans.

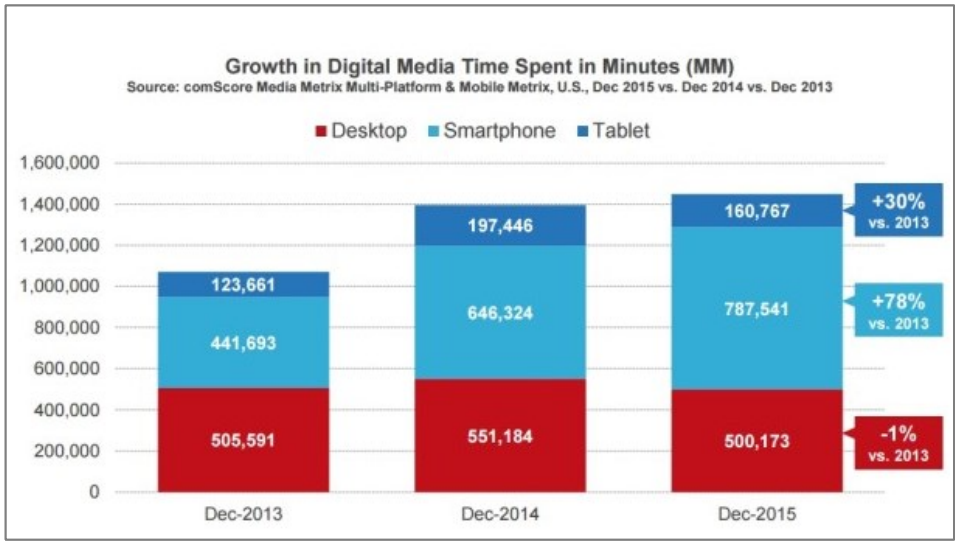
ID n° 18 Marché des Wearables ou internet des objets. Source Gartner

158 Source https://fr.wikipedia.org/wiki/Minitel

159 Animateur du groupe de travail de l'ISO/IEC sur les systèmes de management de la sécurité de l'information. Edward Humphreys est reconnu comme le « père » des normes ISO / IEC 27001 de systèmes de gestion de la sécurité de l'information.

2.3. INTERNET, OUVERTURE VERS LE MONDE OU LE CYBER-ENFER ?

L'accès à internet depuis les ordiphones et tablettes a dépassé celui des ordinateurs en 2016, 88 % du temps passé sur internet, se fait à travers les applications installées sur les appareils mobiles.



ID n° 19 Etude ComScore comparaison du temps passé sur internet à partir de certains médias[160]

Les frontières des systèmes ne sont plus limitées avec l'avènement du Cloud [161]et du BYOD[162] (Bring Your Own Device), ce qui expose les organisations à faire face à de nouveaux risques.

Selon Médiamétrie[163], la France comptait plus de 47,1 millions d'internautes en juillet 2017, soit 90 % des Français. En un an, le nombre d'internautes a augmenté de 3,5 %. La même source indique que 26,5 millions de Français se connectent journellement à un réseau social (Facebook, Messenger ou Twitter), cette activité représente 20 % du temps passé sur internet. Les cybers attaquants visent ces plateformes où ils trouvent de nouvelles victimes ; *Locky* est apparu sur Facebook en 2016.

2.4. RETOUR D'EXPERIENCES

Les bons droits, à la bonne personne au bon moment

Voir la trame du questionnaire Annexe n°15 page 193.

2.4.1. INTERVIEW DE RSSI (RESPONSABLE DE LA SECURITE DU SYSTEME D'INFORMATION)

Des interviews ont été menées auprès de RSSI, contactés via le club de sécurité le CESIN, entre

160 http://www.comscore.com/Insights/Presentations-and-Whitepapers/2016/2016-US-Cross-Platform-Future-in-Focus

161 Le cloud computing, ou l'informatique en nuage ou nuagique ou encore l'infonuagique (au Québec), est l'exploitation de la puissance de calcul ou de stockage de serveurs informatiques distants par l'intermédiaire d'un réseau, généralement internet. Source Wikipédia

162 BYOD, abréviation de l'anglais « Bring Your Own Device » (« apportez vos appareils personnels ») ; est une pratique qui consiste à utiliser ses équipements personnels (smartphone, ordinateur portable, tablette électronique) dans un contexte professionnel. Source Wikipédia

163 http://www.journaldunet.com/web-tech/chiffres-internet

septembre et décembre 2017 et le réseau LinkedIn. Les RSSI qui ont répondu, travaillent dans le secteur privé ou le public. Un questionnaire identique a été utilisé pour l'ensemble des personnes interviewées.

➔ *INTERVIEW DE MONSIEUR CEDRIC CARTAU*

Interview réalisée par téléphone le 17 novembre 2017.

VOUS

- RSSI et DPO du CHU de Nantes,
- RSSI et DPO du Groupement Hospitalier de Territoire 44,
- Travaille dans le monde hospitalier depuis 18 ans,
- Auteur de 2 ouvrages sur les systèmes d'information,
- Enseignant à l'EHESP,
- Chroniqueur dans DSIH Magazine.

PERIMETRE

- Sécurité du système d'information au CHU de Nantes et dans le cadre du GHT
- Formateur sur le système d'information à l'EHESP (école des Hautes études Public en Santé).

METHODE ET APPROCHE

Monsieur Cartau aborde la sensibilisation des utilisateurs avec :

- Des affiches : *les dix commandements de la sécurité informatique*
- Un « *Kit de survie* » est copié sur tous les ordinateurs, comprenant les procédures dégradées des logiciels majeurs,
- Intervention dans les séminaires.

SENSIBILISATION

La sensibilisation à la sécurité des systèmes d'information est très difficile auprès des dirigeants de l'hôpital.

Pour exemple, Monsieur Cartau indique un projet en réflexion sur la mise en place d'un logiciel non sécurisé, traitant de données de patients de son établissement au Maghreb et dont l'éditeur peut accéder à des données médicales. Cette pratique est réprouvée par le RGPD, mais surtout seul un médecin peut accéder aux données médicales.

Une sorte de « *jurisprudence* » s'établit lorsqu'un autre établissement a installé le même type de logiciel dans leur système d'information ; il est difficile de faire entendre raison aux dirigeants de l'hôpital,

Un autre exemple est l'externalisation de la frappe des comptes rendus des patients en Tunisie par des étudiants en médecine.

Monsieur Cartau compare les campagnes de prévention à des accidents de la route et son efficacité. Seul le « *bâton* » fonctionne avec les radars et les points supprimés sur le permis.

Il est difficile de démontrer que les actions mise en place marchent : la sensibilisation ne sert à rien en soit car il suffit d'un seul faux pas pour contaminer tout le réseau ! Un utilisateur clique sur un message malveillant, une pièce jointe (ex : facture reçue au service financier qui est très bien imitée) pour anéantir toute la sensibilisation effectuée.

« La sensibilisation ne sert à rien tant qu'un crash n'est pas arrivé (sensibilisation par la preuve, analyse Post-mortem) ».

50 % des incidents de sécurité du système d'information sont dus à un non-respect des bonnes pratiques de la part des informaticiens. En moyenne un crash tous les 18 mois (exemple : mise en production un vendredi !)

Le système d'information a évolué. Il y a 20 ans, il était demandé une excellence technique aux informaticiens (ultracompétence technique) car l'informatique rentrait à l'hôpital. Maintenant on demande aux informaticiens d'être compétents et de savoir suivre et mettre en œuvre des procédures.

Sur un personnel de 120 informaticiens 1/3 ne comprennent pas le discours de modernisation, qualité et sécurité.

L'hôpital est confronté aux mêmes difficultés que le service qualité il y a 10 ans avec la mise en place des certifications de l'HAS.

Les services qualité ont formé et sensibilisé les personnels soignants ; la même démarche n'a pas été opérée auprès des DSI et des informaticiens.

Les Directeurs d'établissement de plus de 35 ans n'ont pas été formés au système d'information à l'EHESP (école des Hautes études Public en Santé). Ils reçoivent une formation de gestionnaire (comptable) d'établissement de santé uniquement.

Depuis 2013, les dirigeants ont un « vernis » de deux jours, sur l'ensemble de leur cursus, sur le système d'information (pilotage des systèmes d'information). Ces professionnels ont conscience de la défaillance de cette formation, mais arrivés dans la vie active, ceux-ci ont occulté leur réflexion initiale et prennent des décisions parfois absurdes concernant le système d'information (exemple : construction d'un bâtiment sans consultation de la DSI).

En 2007, sur une promotion de 60 personnes, seules 10 choisissait une spécialité IT.

Malheureusement, il n'y a pas de réflexion sur les erreurs passées afin de progresser (roue de Deming inexistante).

Donc, les utilisateurs seront catégorisés et sensibilisés en conséquence : Utilisateurs, Direction et système d'information. Les utilisateurs sont les acteurs les plus sensibles aux campagnes de sensibilisation.

Monsieur Cartau suggère la mise en place d'un « *passeport système d'information* » comme aux USA. Une formation aux outils métiers et informatiques est effectuée en présentielle ou en formation en ligne ou les deux auprès des acteurs de l'établissement de santé. Les acteurs sont habilités à accéder au système d'information que s'ils ont le nombre de points requis.

Difficulté de communication avec les RH, concernant les remplacements. Les personnels recrutés ne suivent pas de formation, alors que cette gestion de vivier de remplacement devrait être effectuée comme dans le privé et ces personnes formées. Les RH avancent des arguments comme quoi cela a un coût, mais le coût de la non-formation, sans compter des incidences sur le dossier patient, est encore plus élevé.

SUPPORT

À votre avis, quel est le meilleur support de diffusion de message et pourquoi :

- Clip vidéo, car c'est un support attrayant.
- Affiches, car ces supports peuvent être renouvelables et disposés aux endroits stratégiques. Celles-ci suscitent aussi des échanges, à la machine à café par exemple.

CONCLUSION ET ANALYSE DE L'INTERVIEW

Monsieur Cartau, est un professionnel de la sécurité de l'information dans le domaine hospitalier. Son avis est assez pessimiste, quant à la prise en compte de la sécurité par les Dirigeants des établissements de santé.

Son approche de la sensibilisation auprès des agents ou des futurs dirigeants, se veut pédagogique (affiche, vidéo, formation à l'école des Hautes études Public en Santé).

La piste à retenir est le *Passeport Sécurité* comme aux états unis.

➔ *INTERVIEW DE MONSIEUR CHRISTIAN CEVAËR*

Interview réalisée en face-à-face le 30 octobre 2017

VOUS

- Responsable Sécurité du Système d'Information - Direction du Pilotage du Système d'Information Chambre de commerce et d'industrie de région Paris Ile-de-France.
- J'ai commencé par l'activité de développeur, administrateur système pour évoluer vers un poste de RSI d'une unité de 200 personnes. J'ai travaillé dans une SSII spécialisée dans l'audiovisuel.
- Je suis passé chef de projet et ai intégré la CCI Paris comme Responsable solution utilisateurs.
- J'ai été également responsable d'exploitation téléphone, réseau, système et web
- La CCI gère 180 sites, soit, environ 8 000 personnes (sans les étudiants)
- Je n'ai pas de formation spécifique en sécurisation de l'information.
- J'ai passé un certificat professionnel de responsable RSSI FCP dans un centre de formation agréé et ai suivi une formation de trois semaines à Orsys.
- Enfin, en novembre 2015 j'ai été nommé RSSI auprès de la CCI. Le poste était inoccupé depuis un an et il n'y avait pas de Politique de sécurité des systèmes d'information mis en place.
- Je suis nommé pour la CCI Paris et Ile-de-France
- Cela représente 19 écoles (Ferrandi, Gobelins, Meissier…)

PERIMETRE

- Sensibilisation, analyse de risques, audits, gestion des incidents de sécurité, accompagnement au projet (Chef de projet, MOA, MOE), administratif (clause, et analyse des réponses aux marchés).
- La CCI n'a pas de CIL (Correspondant informatique et liberté) ; un DPO[164] sera nommé en interne.

[164] En droit européen, le Délégué à la protection des données (abrégé DPD, ou DPO, pour Data Protection Officer) est la personne chargée de la protection des données au sein d'une organisation. Source Wikipédia

METHODE ET APPROCHE

J'utilise le courriel pour :

- Diffuser de l'information générale sur les bonnes pratiques une fois par trimestre,
- Communiquer sur des alertes auprès des utilisateurs et de la DSI,
- Communiquer les alertes du CERT et avis auprès des personnes concernées. Les équipes de production regardent leurs alertes en provenance des éditeurs, le CERT (Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques français) est le garde-fou.

J'interviens en présentiel toutes les semaines :

- Auprès des rendez-vous filières : rendez-vous par métiers (exemple : les webmasters)
- Sous forme de conférence avec des messages correspondants à la filière toutes les semaines,
- En Codir par direction de chaque école, afin de confronter les risques/métiers
- En Comex (constitué de l'équipe du Codir et des élus)
- J'organise des conférences en ligne (*webinar*) une fois par mois et une conférence de 30 minutes sur la sécurité tous les deux mois.

Depuis 2016 la CCI a mis en place le télétravail : j'interviens pendant les formations des télétravailleurs sur des points de sécurité. Les personnes souhaitant exercer en télétravail ont une obligation de suivre cette formation.

Les supports sont diffusés sur l'Intranet, comme la PSSI, les guides ciblés par population, le guide général des bonnes pratiques et un bulletin d'information spécialisés sécurité de l'information.

SENSIBILISATION

La mixité des moyens, des supports et des méthodes est la seule solution pour sensibiliser les acteurs de la CCI.

Je réalise des campagnes de phishing et mesure les retours de clics.

J'ai budgété des tests intrusion pour l'année 2018.

J'oriente la sensibilisation en prenant des exemples sur la vie privée.

Le Shadows IT est abordé également, en expliquant les risques encourus pour la CCI et les données personnelles des utilisateurs.

Je rebondis sur des cas concrets de l'actualité du moment, qui met en situation le risque.

Le support de proximité remonte les incidents de sécurité via le logiciel de ticketing auprès du RSSI, qui les traite.

J'accompagne les chefs de projets avec des outils comme le QERSI-S (Questionnaire d'évaluation des Risques pour le Système d'Information de Santé)[165], des questionnaires de maturité (ANSSI), un PAS (Plan d'Assurance Sécurité) est également utilisé.

Les chefs de projets sont demandeurs de bonnes pratiques en matière de sécurité.

Je me positionne comme « *Apporteur de solution et non de contrainte* », et j'emploie l'humour auprès

---

[165] Questionnaire, réalisé par le GCS TéléSanté Centre et l'APSSIS, à partir du questionnaire initial de la CNAM-TS. Cette grille permet d'analyser les risques qu'un système fait porter à un établissement de santé. https://www.apssis.com/upld/fichiers/Questionnaire-QERSI-S-v2.pdf www.sante-centre.fr

des utilisateurs afin de dédramatiser la situation.

J'ai une technique lors de mes interventions est de faire monter le stress dans l'assistance avant de faire redescendre la pression avec quelque chose de léger.

SUPPORT

- L'Intranet (diffusion d'informations d'actualité, des guides de bonnes pratiques, des contacts, des alertes sur les menaces).
- Un bulletin d'information sécurité adressée aux utilisateurs / à la direction
- Des courriels ciblés ou ponctuels suivant l'actualité
- Des campagnes de courriels de type phishing pour tester la réaction des utilisateurs
- Intervention dans les réunions (Codir, réunion de cadres, réunion avec les syndicats, réunion hebdomadaire d'équipe etc.)
- Formation des utilisateurs en présentiel par vous-même ou un intervenant extérieur
- Formation en ligne
- Produire de la documentation (la documentation utilisateur qui accompagne les logiciels etc. Mentionne les risques principaux encourus vis-à-vis de la protection des informations, les points de vigilance pour l'utilisateur et les recommandations types à mettre en œuvre).

AUTRES COMMENTAIRES (LIBRE)

Il est important, pour le RSSI d'être légitimé par la Direction et ne pas être attaché à la DSI, car il peut y avoir des conflits d'intérêts. Il est difficile de faire appliquer des actions contraignantes, sans l'appui de la Direction.

La sensibilisation devrait être prise en compte dans le budget de la CCI (campagnes de phishing, des bulletins d'information et le temps homme nécessaire pour ces réalisations).

Les administrateurs des systèmes d'information devraient, obligatoirement suivre des formations sur la sécurité appliquée à leurs domaines, dont le piratage informatique.

Il est important que le RSSI adhère à un club ou, une association, afin d'échanger avec ses pairs. Je suis adhérent du CLUSIF. Je me rends aux réunions mensuelles et participe aux groupes de travaux.

CONCLUSION ET ANALYSE DE L'INTERVIEW

Monsieur CEVAËR, ne ménage pas son temps et son imagination pour sensibiliser les différentes populations sous la tutelle de la CCI. Il utilise presque tous les supports pour faire passer son message.

Nous retiendrons que le statut du RSSI sera légitimé s'il est attaché à la Direction si s'il a les moyens nécessaires pour asseoir son autorité en matière de sécurité.

Les personnels de DSI doivent être particulièrement sensibilisés et suivre des formations adéquates ; connaître son ennemi est le premier pas vers la protection des informations.

2.4.2. INTERVIEW DE RESPONSABLE DE LA SENSIBILISATION DES ACTEURS DE L'ORGANISATION

M. Fabrice NERACOULIS, Responsable de la sensibilisation de la SNCF (150 000 personnes). Réseau SSI / Attitude 3d – direction générale e-SNCF - direction production informatique et télécoms - Pôle Cyber sécurité (5 septembre 2017 face-à-face).

VOUS

- Pilote de la sensibilisation de la SNCF depuis 7 ans.
- La cellule de sensibilisation est née en 2008.
- Attitude3D s'appuie sur un réseau de 50 animateurs SNCF. Ces intermédiaires participent à la distribution de gadgets, matériels…
- La difficulté de faire appel à des intermédiaires, est la distorsion des messages portés.
- Monsieur Néracoulis ne parle pas de sécurité mais de protection de l'information.

PERIMETRE

- Le périmètre est uniquement la sensibilisation à la sécurité de l'information. Les moyens techniques sont assurés par la DSI de la SNCF.

METHODE ET APPROCHE

Les méthodes de science cognitive permettent de toucher les utilisateurs, éveiller leur conscience à la sécurité. Les utilisateurs doivent être engagés.

Je conseille la lecture du « Petit traité de manipulation à l'intention des honnêtes gens » de Robert Vincent Joule et Jean Léon Beauvois. « *Mettre un pied dans l'écran* » à l'instar du commercial qui, peut mettre le pied dans la porte afin de forcer l'attention de son client deviendra une seconde nature.

SENSIBILISATION

L'étude de la SNCF est en Annexe n°14 page 189.

Les serious game ont un coût élevé et un impact de seulement 1 %, les utilisateurs adhèrent difficilement car « *ils viennent au bureau pour travailler et non pour jouer !* ».

Les vidéos de la *Hack Académie* [166] sont visionnées en réunions suivies d'un compte rendu général.

Les utilisateurs aiment les questionnaires. 30 000 personnes ont participé au questionnaire 2016 sur 150 000 salariés de la SNCF ; un iPad était en jeu.

Le livre blanc de « La défense et de la sécurité nationale »[167] réédité en 2013, indique que les attaques informatiques sont en deuxième position après les risques terroristes.

SUPPORT

Les médias seront adaptés à la population (post-it, tapis de souris, etc.) et améliorer les techniques de communication. L'approche sera ludique (voir Annexe n°14 page 189).

[166] https://www.hack-academy.fr/
[167] www.livreblancdefenseetsecurite.gouv.fr/

ID n° 20 support de communication de la sécurité

La SNCF édite des bandes dessinées thématiques et ciblées, qui sont rassemblées dans un seul ouvrage en fin d'année. Ces recueils ont beaucoup de succès auprès des acteurs de l'organisation.

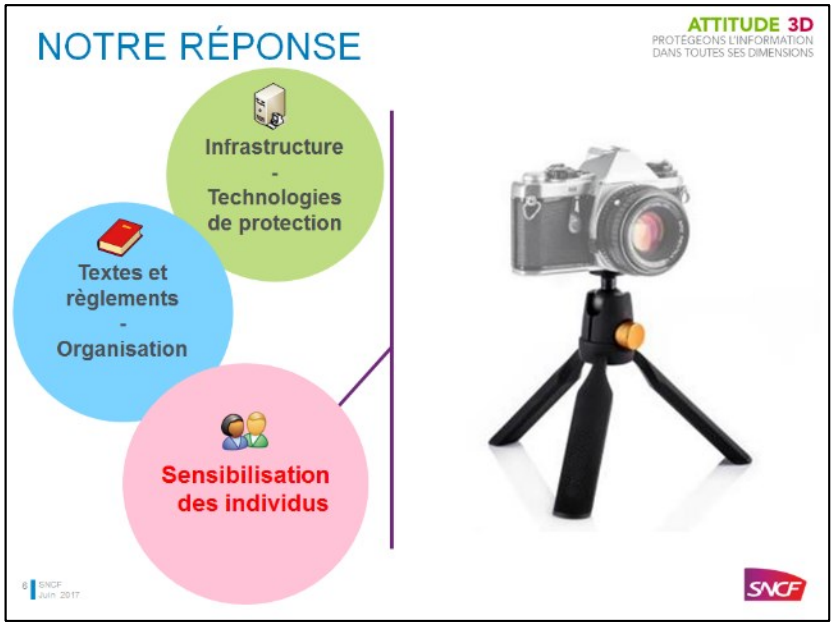
Le budget d'Atitude3D est de 1 € par agent et par an. La SNCF représente 150 000 salariés.

Les calendriers ont un *rapport « efficacité prix »* intéressant. Celui-ci est vu par un nombre conséquent de personnes, car le calendrier est à la vue de tous dans le bureau. Un message différent est diffusé par mois.

IDENTITE

Une identité spécifique a été donnée à cette organisation : *Attitude3D*.

Attitude3D symbolisé par le trépied d'un appareil photo



ID n° 21 symbolisation d'Attitude3D.

CONCLUSION ET ANALYSE DE L'INTERVIEW

Monsieur Néracoulis est un défenseur de la protection de l'information. Il n'a pas du tout de démarche technique et a saisi que les acteurs de l'organisation seront « *utilisés* » comme des boucliers devant la cyber criminalité.

Chaque année, l'imagination de Monsieur Néracoulis pousse l'usage de nouvelles approches, ludiques, pour sensibiliser les utilisateurs.

Le projet de l'année 2018 est une immersion 3D avec un ordiphone, dans une scène où des dangers sont disséminés dans un bureau. Comme le jeu des 7 erreurs, interactif.

L'approche à retenir ici, est l'étude du ROI des différents supports de la sensibilisation et l'approche ludique (bandes dessinées, ordiphone).

2.4.3. ENQUETE AUPRES DE PROFESSIONNELS DE LA SECURITE

Le détail des résultats de l'enquête est Annexe n°18 page 195.

➔ *QUI SONT LES REPONDANTS*

Le questionnaire a été posté sur internet, entre le 8 juillet et le 10 novembre 2017, auprès de personnes, professionnelles de la sécurité et des systèmes d'information.

Il y a eu 207 réponses, 38 réponses ont été éliminées de l'étude car trop incomplètes, donc nous avons exploité 169 réponses.

Sur ces 169 réponses, 55,03 % des répondants sont RSSI (Responsable de la Sécurité des Système d'Information), du domaine public (63 %) et du privé (37 %). Le secteur économique le plus représenté est celui de la santé (25,44 %), de la finance (13,16 %) et du Conseil et services (8,77 %).

Les entreprises sont situées essentiellement à Paris (52,38 %) et loin derrière à Marseille (2,38 %).

Leur taille se situe entre 500 et 2 000 employés pour la majorité (8,33 %)

➔ *CE QUI EST A PROTEGER*

Il est paradoxal de constater que l'évaluation des risques a été menée sans prendre en compte les risques de pertes financières (55 %). Malgré ce point, une stratégie de sécurité a été formalisée.

Les commentaires apportés, permettent de nuancer les réponses : les risques sont évalués en « *grosses mailles* » ou sur les sujets les plus sensibles de l'organisation. Des difficultés de dimensionnement des équipes sécurité sont également indiquées ; ce qui explique l'identification des risques partiels (majeurs) par manque de main-d'œuvre, ou de moyen, pour mandater un prestataire externe. Pour certains un audit de sécurité est en cours.

63 % des RSSI qui ont répondu au sondage, sont issus du domaine public ; cette notion de perte financière semble absente des réflexions de sécurisation des systèmes d'information. 83 % des RSSI du service public disent traiter des données sensibles.

Pourtant, les données de santé sont une mine d'or pour les pirates qui attaquent les établissements de santé et leur demande des rançons. L'aspect financier, dans ce cas, devient rapidement concret. Sans compter « *le manque à gagner* » car les patients s'orienteront vers d'autres établissements, de même type offrant plus de sécurité à leurs données personnelles, si celles-ci sont corrompues et jetée sur la place publique.

La méthode d'analyse de risque Ebios est la plus couramment utilisée. La méthode EBIOS est une

méthode d'évaluation des risques en informatique, créée en 1995 par la Direction centrale de la sécurité des systèmes d'information (DCSSI) et maintenue par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) qui lui a succédé en 2009.

➔ *LES TIERS*

Les partenaires et prestataires sont pris en compte dans la sécurité.

Un Plan d'Assurance Sécurité (P.A.S) est mis en place pour 56 % des organisations. Des progrès sont encore à accomplir sur ce sujet. La mise en place du RGPD, va pousser les organisations à prendre en compte les personnes externes.

➔ *LA SECURITE DANS LES PROJETS*

Les RSSI ont saisi l'importance de la prise en compte de la sécurité dans les projets, car 71 % interviennent en amont et 65 % pendant le projet.

Malgré cette prise de conscience, l'analyse de risque est peu (34 %) formalisée au travers d'un document standardisé.

➔ *SMSI*

Le corollaire de la norme ISO 27 est utilisé pour plus de la moitié des organisations qui ont répondu (voir 2.5.3 page 79 pour plus de détail sur la norme ISO).

Cette norme est exhaustive. Elle prend en compte tous les paramètres d'une organisation, de la sécurité de l'information et est reconnue mondialement.

➔ *LE RGPD*

Le RGPD (voir §2.5.1 page 78), apporte des modifications conséquentes à la politique de sécurité en place dans les organisations, pour protéger les données à caractère personnel.

Fin novembre 2017, les organisations privées étaient mieux informées (79 %) que les organisations publiques (48 %). Les entreprises privées n'étaient pas prêtes, pour autant, à la mise en conformité avec le RGPD : 31 % n'avaient pas lancé le chantier de mise en conformité.

Paradoxalement, le secteur public, bien que moins informé a lancé le projet de mise en conformité du RGPD avec un taux de préparation à 25 % pour 38 % des répondants fin novembre 2017.

Leur marge de progression est importante vis-à-vis du privé. 7 % du secteur privé atteint 75 % de taux de préparation, à comparer avec le public qui lui est à 14 %.

➔ *LES SUPPORTS UTILISES POUR SENSIBILISER LES ACTEURS DANS LE DOMAINE PRIVE ET PUBLIC*

Les commentaires apportent une lumière supplémentaire sur le choix des supports. Dans la grande majorité des cas, les répondants n'ont pas de « recette miracle », ce qui fonctionne est la constance des messages, la combinaison des méthodes que l'on adaptera aux interlocuteurs suivant leur âge et leur centre d'intérêt.

Le mot « *Serious game* » est très présent dans les commentaires annexes. Ceux-ci sont sécables, « *les modules en ligne sont répartis dans le temps et permettent d'assurer une sensibilisation continue* ». Ils sont « *ludiques* » et « *incitatifs* », s'ils sont couplés avec des lots suivant la note finale de l'apprenant. La standardisation de ce support à fait baissée leur coût, donc cette sensibilisation est devenue « *rentable* ».

L'approche directe ou choc est privilégiée pour faire passer des messages ciblés ou chocs (séance de piratage en direct par exemple, compte rendu sur un film – Hack académie — montrant des pirates informatiques en action ou leurs conséquences, voir Annexe n°14 page 189).

2.4.4. ENQUETE AUPRES DES ACTEURS DE L'ORGANISATION

Le détail des résultats de l'enquête est Annexe n°19 page 206.

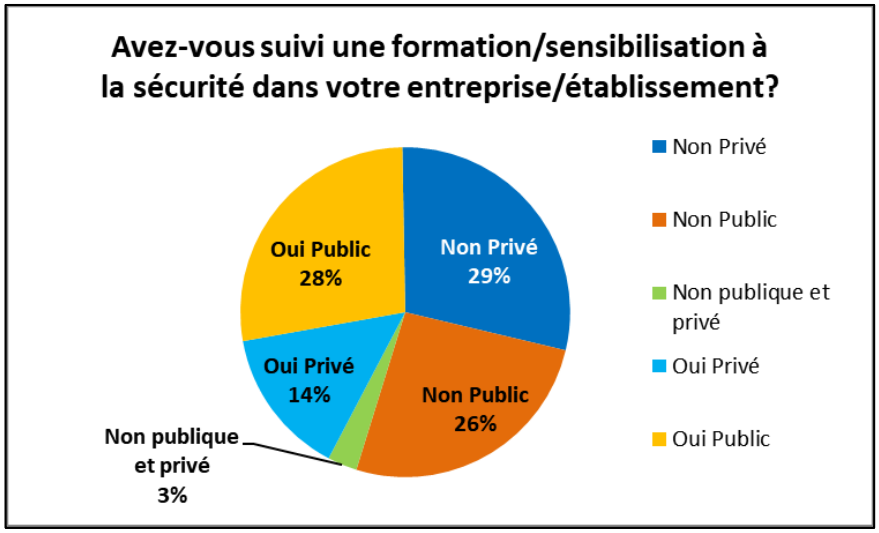
➔ *QUI SONT LES REPONDANTS*

Le questionnaire a été posé sur internet, entre le 8 juillet et le 10 novembre 2017, auprès de personnes, non professionnelles de la sécurité des systèmes d'information et utilisant un ordinateur. Il y a eu 78 réponses, 9 réponses ont été éliminées de l'étude car trop incomplètes (2 champs renseignés sur 94).

Un équilibre apparaît dans la répartition des réponses au niveau du secteur privé 43 % et publique 54 %, issues essentiellement du milieu de la santé 44.93 %.

Presque la totalité des répondants ont un ordinateur (99 %), équipé d'un antivirus (84 %).

La majorité (58 %) des personnes, indique ne pas avoir été sensibilisée à la protection de l'information, dans leur organisation. Les réponses sont proches dans le camp des « Non » dans le privé (29 %) et le public (26 %), en revanche les personnes du domaine public (28 %) affirment avoir été plus sensibilisées que dans le privé (14 %).

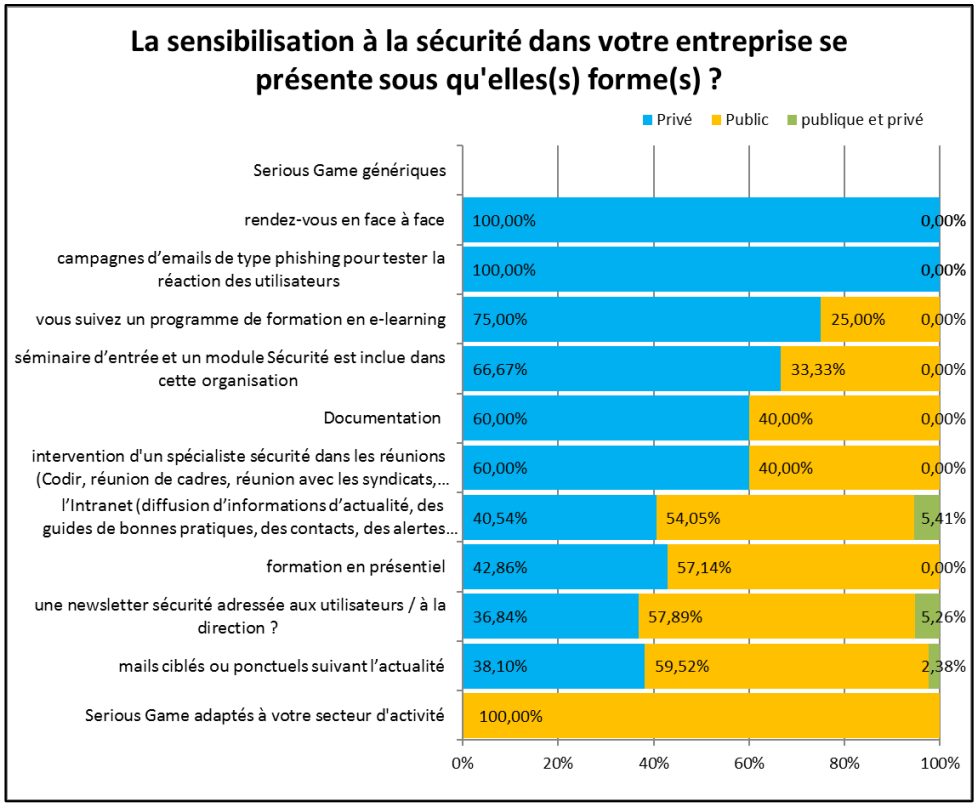


ID n° 22 Avez-vous suivi une formation/sensibilisation à la sécurité dans votre entreprise/établissement ?

➔ *LES SUPPORTS UTILISES POUR SENSIBILISER LES ACTEURS DANS LE DOMAINE PRIVE ET PUBLIC*

Le secteur privé privilégie, l'approche directe (réunion en face-à-face et séminaire d'entrée), les campagnes de phishing de courriel et la formation en ligne.

Le secteur public se comporte à l'inverse, en donnant la priorité au serious game adapté au secteur d'activité, aux courriels ponctuels, aux bulletins d'information et aux formations en présentiel.



ID n° 23 Résultats "sous qu'elle forme se présente la sensibilisation dans votre organisation ?

➔ *À LA QUESTION « SELON VOUS QU'ELLES SONT LES METHODES LES PLUS EFFICACES, CELLES QUI VOUS ONT LE PLUS MARQUEES ET AVEZ-VOUS RETENU DES ACTIONS QUE VOUS AVEZ APPLIQUEES ? »*

Les réponses sont troublantes vis-à-vis des réponses choisies dans les questionnaires :

> *Vu les questions, dans ma boîte nous sommes « à la ramasse » les campagnes de courriel type phishing me paraisse une excellente idée la formation en présentielle tous les ans ou tous les 2 ans seraient bien aussi… Après c'est le problème du temps. La doc ! Ils ne la lisent pas sauf sous forme formation accompagnée de QCM d'évaluation (formation en ligne).*
>
> *Qu'est-ce qu'un serious game ? Le titre est alléchant !*
>
> *Corinne, Analyste développeur*

Globalement les personnes n'ont pas l'air très sensibilisées, elles suivent des bonnes pratiques (ce qui est déjà bien !) consultent des documentations spécialisées à leur pratique professionnelle :

> *Diffusion d'informations d'actualité, des guides de bonnes pratiques, des contacts, des alertes sur les menaces. Olivier, Graphiste*
>
> *Je lis les bulletins d'information qui traitent du sujet : par exemple la Newsletter du ministère de l'économie adressée aux entreprises. Christine, Avocate*
>
> *Suivre les instructions, ne pas ouvrir de courriels inconnus. Pour le reste, je fais confiance aux professionnels sécurité de l'entreprise. Marc, Adjoint Responsable d'exploitation*
>
> *Toute petite structure, rien de formel sur la sensibilisation. Plutôt des alertes données à l'occasion, et une culture générale de bonnes pratiques informatiques partagée. Sarah, Directrice de projet*

Certaines organisations, oublient la sensibilisation et appliquent des restrictions majeures sur les postes des utilisateurs, qui de toute façon, à un moment ou un autre trouveront une parade pour

travailler avec les outils qui leur sont nécessaires. YouTube est de plus en plus utilisé pour la diffusion d'informations professionnelles comme des tutoriels.

> *Il n'y a pas si longtemps sur notre hôpital, tout pouvait se télécharger ! À ce jour présence pour accéder à un serious game sur mon secteur d'activité, je dois demander au service informatique de me le télécharger, car c'est sur YouTube, un site non sécurisé. Il en est de même pour des vidéos sur le thème hygiène en milieu hospitalier disponible sur ce même site, je le fais télécharger par le service informatique. Il n'y a plus d'accès USB.*
>
> *Nadine, infirmière hygiéniste*

Ou certains pratiquent le jeu de « *big brother* » ! « *Nous savons tout sur vous !* »

> *Le responsable SSI de l'unité s'est mis sur mon ordinateur pour vérifier que j'appliquais bien les consignes. C'est impressionnant de voir qu'il peut tout savoir sur mon ordinateur ! (Bon, je n'avais rien à me reprocher mais c'était pour l'exemple pour les autres).*
>
> *Caroline, chargé d'études*

2.4.5. INTERVIEW DE MADAME VIARD, CONSULTANTE SENIOR CHEZ WAVESTONE CABINET DE CONSEIL EN SECURITE

Interview réalisée le 14 septembre 2017 par téléphone.

Wavestone est née en 2016, fruit du rapprochement de deux cabinets établis et reconnus, cette société exploite plusieurs décennies d'expérience dans des univers différents mais complémentaires : le monde du conseil en management et celui du conseil en digital et innovation technologique. Cette entreprise est reconnue sur le secteur de la sécurité pour la qualité de ses interventions.

➔ *VOUS*

- Madame Viard est consultante Sénior chez Wavestone depuis 5 ans. Elle est ingénieur télécoms avec une spécialisation en système réseau et à découvert la sécurité pendant ses études.

➔ *PERIMETRE*

- Ses activités s'étendent sur le secteur privé et public.
- Ses interventions concernent la gouvernance de la sécurité, la PSSI, les conformités réglementaires, LPM, PDSI et l'organisation de la sécurité en passant par la sensibilisation, la mise en place de PRA/PCA et la gestion de crise.
- Les aspects techniques sont pris en charge par des experts internes à Wavestone ou les équipes locales des clients.

➔ *METHODE ET APPROCHE*

- Nous abordons la sécurité par un tronc commun pour tous les utilisateurs.
- Nous identifions les personnes particulièrement ciblées par la cyber délinquance et organisons des campagnes de sensibilisation en fonction de leur activité et les risques relevés. Les actions sont adaptées aux acteurs (COMEX, CODIR, top management, etc.).
- Nous réalisons des opérations coup de poing ; exemple pour des ordinateurs non attachés par câble, nous identifions les postes et collons un message sur l'écran.
- L'approche de la sensibilisation est dépendante du budget, du temps que les utilisateurs auront à y consacrer et des messages à faire passer.

➔ *SENSIBILISATION*

La mesure de la sensibilisation apportée est mesurée directement « *à chaud* » en fin de session,

ou formation en ligne pour comprendre si les messages sont compris ou non.

Nous mettons en place des indicateurs et réalisons des audits. Par exemple le suivi du marquage de la confidentialité, nous prenons des échantillons de documents et les analysons. Nous pouvons également compter combien d'ordinateurs sont attachés au bureau, tous les mois, etc.

La formation en ligne a un fort impact, car il y a plus de messages diffusés. Une personne reste en moyenne 20 minutes devant son écran, et peut aborder plusieurs thématiques.

Nous travaillons avec le service de communication des entreprises, qui s'appuie sur leur expérience, pour délivrer les messages aux employés et, les graphistes pour créer des documents attrayants.

Nous travaillons avec des partenaires pour les bandes dessinées, les vidéos de sensibilisation et des éditeurs de solutions de formation en ligne.

➔ *SUPPORT*

Il n'y a pas de matériels idéaux, tout dépend du budget et du message que l'on veut faire passer.

Le « *coût/efficacité* » sera à étudier.

Par exemple les opérations coup de poing ne sont pas chères car il s'agit seulement du temps du RSSI (exemple : ramasser tous les ordinateurs portables qui ne sont pas attachés le soir).

L'état des menaces en COMEX (30 minutes environ) ne coûte pas cher.

On peut également utiliser des solutions de formation en ligne toutes prêtes pour délivrer des messages génériques. Leur inconvénient est que l'on ne peut pas les personnaliser.

➔ *IDENTITE*

J'ai rarement vu une charte visuelle sur un service en entreprise comme c'est le cas à la SNCF. Une personne spécialement dédiée à la sensibilisation en entreprise est rare.

➔ *ORGANISATION*

Le RSSI est à 50 % attaché à la Direction et le reste du temps à la DSI.

Il peut y avoir des conflits d'intérêts avec la DSI et le responsable de la production, qui, pour assurer le service, tentera de passer outre la sécurité.

L'inconvénient d'être attaché à la Direction est d'avoir une moins bonne connaissance de la DSI et des projets en cours et à venir.

➔ *PROJET*

Nous intervenons à tous les stades d'un projet. Nous sensibilisons le chef de projet afin d'intégrer la sécurité dans les projets.

Nous analysons rapidement le projet, afin de déterminer sa sensibilité et s'il est nécessaire de mener une étude de risque approfondie.

➔ *ECONOMIE*

Les entreprises ont recours aux cyber assurances (n'a pas de chiffres).

➔ *AUTRES COMMENTAIRES (LIBRE)*

La sensibilisation des acteurs est primordiale.

L'ingénierie sociale se développe de plus en plus. Les utilisateurs sont attentifs aux courriels qu'ils reçoivent et, les campagnes de phishing font moins de victimes.

Il est indispensable, de mettre des mesures techniques en place, en complément des actions de sensibilisation.

2.4.6. SUIVI DE L'ACCOMPAGNEMENT ET DE LA MISE EN PLACE D'UNE STRATEGIE DE SENSIBILISATION

➔ *L'ORGANISATION ACCOMPAGNEE : SOCIETE CARMIGNAC, GESTIONNAIRE D'ACTIFS*

Fondée en 1989 par Edouard Carmignac et Éric Helderlé en France, Carmignac. Il s'agit d'une Société Anonyme de 300 employés avec un capital de 15 000 000 €, d'un chiffre d'affaires de 819 170 250 € en 2015 et l'un des principaux acteurs européens de la gestion d'actifs financiers. Les fonds Carmignac sont à présent distribués dans 12 pays européens, dont l'Italie, l'Allemagne, l'Espagne, le Royaume-Uni. La sécurité est tout à fait intégrée au sein de cette entreprise, du fait du métier qu'elle exerce et les risques qu'elle peut rencontrer.

Monsieur KELES est RSSI, à plein temps, de la société Carmignac depuis 2015, a un cursus de base technique (Administrateur système et réseau), a suivi une formation qualifiante de RSSI chez Cap Gemini et auprès de l'ANSSI. Il est certifié ISO 27001.

M. Önder KELES, Information System Security Manager. Carmignac (gestionnaire de fonds de placement) http://www.carmignac.com/ (7 septembre 2017 face-à-face)

Une gouvernance de la sécurisation de l'information a été mise en place au sein du cabinet.

Le RSSI est placé sous l'autorité du Directeur des opérations et peut ainsi avoir du poids dans les actions à mener. Les objectifs généraux sont validés par la Direction générale.

Des relais sont mis en place dans les services auprès des métiers, qui sont le mieux à même de déterminer la sensibilité des informations qu'ils traitent et comment les classifier. Le responsable de département est garant de la sécurisation des informations sur son périmètre et il nomme des « référents sécurité » dans son département, qui est chargé, entre autres de diffuser la bonne parole et les pratiques adéquates en matière de protection de l'information, suivant les directives mises en place dans le cabinet.

Monsieur KELES s'appuie également sur le service de communication du Cabinet, pour éviter des coûts externes, car le service connaît bien les acteurs de l'entreprise et sait comment toucher les personnels. Il fait appel, également aux équipes techniques internes.

Une politique de sécurité du système d'information a été élaborée avec le cabinet et mise en œuvre au sein du cabinet, relayée par les responsables de chaque département.

Une campagne de sensibilisation a été menée auprès des cadres et un audit de la sécurité en 2016. À la suite de cet audit, un plan d'action et des KPI ont été définis pour mesurer l'avancement de la progression de la sécurisation.

Des échanges réguliers sont menés avec Monsieur KELES dans le cadre de ce mémoire, afin de suivre l'avancée de sa démarche.

La première campagne de sensibilisation a commencé le 2 janvier 2018.

Echange avec M. KELES

> *Concernant la mesure de l'efficacité, je compte mener des audits surprise (ex : circuler dans les locaux afin de contrôler les postes non verrouillés, publier de faux liens malicieux, laisser traîner des clefs USB contenant un message d'alerte ainsi qu'une copie de la présentation,)*
>
> *Par ailleurs j'envisage de mener un mini-sondage sur un échantillon de la population.*
>
> *De manière générale, je constate que des personnes, pas du tout concernées par la sécurité IT, s'y intéressent surtout lorsque je retire certains de leurs privilèges, par-ci par-là. Dernier exemple : blocage des ports USB sur les ordinateurs fixes et portables.*
>
> *En plaçant la contrainte en face d'une menace (on interdit cela en raison du risque suivant) on arrive à capter l'attention de l'utilisateur. J'en profite alors pour présenter brièvement les prochaines mesures à venir et les risques associés. J'essaie d'inclure des exemples de tous les jours dans le débat afin d'illustrer mes propos.*
>
> *La difficulté réside dans le fait que l'utilisateur peut, très vite être démotivé, à l'utilisation des technologies qui, jusqu'ici étaient des outils d'aide et de facilité.*

➔ *L'ORGANISATION ACCOMPAGNANTE : LE CABINET CONSEILS WAVESTONE*

(Voir §Interview de Madame Viard, consultante Sénior chez Wavestone Cabinet de conseil en §2.4.5 page 75). La société Carmignac, a souhaité se faire accompagner du cabinet Wavestone dans sa démarche de sécurisation de son système d'information et, pour la campagne de sensibilisation des utilisateurs.

2.5. NORMES, REGLEMENTATION ET BONNES PRATIQUES

2.5.1. CNIL, GDPR OU RGPD

L'union européenne a travaillé pendant quatre ans, à la finalisation du RGPD, afin de prendre en compte les évolutions numériques et, protéger les données à caractère personnel des citoyens européen. Un cadre juridique unifié permet aux entreprises européennes de renforcer la sécurité des données personnelles. Le règlement est applicable depuis le 25 mai 2018[168].

Le RGPD apporte une vision globale de la protection de l'information.

Le RGPD a un fort impact sur les processus de travail qui régissent la gestion des données critiques de l'entreprise et des services comme la DSI, la DRH, le service de communication, etc. Cette nouvelle norme peut être prise comme une chance afin de remettre à plat les processus de l'organisation. Au fil du temps la protection de l'information a été menée au rythme des contraintes réglementaires ou de l'écosystème (prolifération des actes de pirates informatiques).

L'objectif de l'UE est de permettre un meilleur contrôle des données personnelles sur des sujets tels que l'accès aux données, leur portabilité, le « droit à l'oubli » et la possibilité d'être informé en cas de piratage de ses données personnelles dans un délai de 72 heures.

2.5.2. NORME ISO/IEC AWI 15408-1 OU DICT OU CRITERES COMMUNS ET NORME ISO 27002

Ce référentiel est issu d'une collaboration entre le Canada, les Etats-Unis et l'Europe dont le nom complet est « Common Criteria for Information Technology Security Evaluation ». En français, on emploie souvent l'expression Critères communs.

> *Les critères communs sont un guide servant de référence pour le développement et le contrôle de produits et systèmes de l'information manipulant des données personnelles.*

[168] https://www.cnil.fr/fr/plus-de-droits-pour-vos-donnees

> *Les produits contrôlés sont ceux collectant, transportant et manipulant ces données, à savoir des réseaux informatiques, des systèmes d'exploitation, des systèmes distribués et des applications. Un système sera évalué en fonction de l'usage pour lequel il est dédié. Il devra répondre à deux catégories d'exigences de sécurité : exigences fonctionnelles et d'assurance.*[169]

Ce référentiel concerne la divulgation nuisible du bien à des destinataires non autorisés (perte de *confidentialité*), un dommage provoqué au bien par une modification non autorisée (perte d'*intégrité*) ou un déni d'accès au bien (perte de *disponibilité*) et s'adresse aux utilisateurs finaux, aux développeurs et aux évaluateurs.

Le référentiel est constitué de onze classes concernant chacune un domaine, lui-même sous-découpé en familles contenant un ensemble de composants qui corresponde à une exigence de sécurité. Chaque classe a un nom unique dont l'abréviation est constituée de trois caractères Fxx : *F* pour classe d'exigence Fonctionnelle et *xx* pour identifier le nom de la fonctionnalité couverte. Chaque menace potentielle est classée en fonction de pouvoir de nuisance envers les biens à protéger.[170]

2.5.3. ISO/CEI 27002

La norme internationale ISO/CEI 27002 concerne la sécurité de l'information. Elle a été publiée conjointement en 2005 par l'Organisation internationale de normalisation ISO et la Commission électrotechnique Internationale IEC, révisée en 2013. Le nom de la norme en français est *Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information*. Elle fait partie de la suite ISO/CEI 27000.

L'ISO/CEI 27002 est un ensemble de 114 bonnes pratiques (nommées « best practices ») à destination des responsables de la mise en place ou du maintien d'un Système de Management de la Sécurité de l'Information (SMSI). La protection de l'information est définie comme la « préservation de la confidentialité, de l'intégrité et de la disponibilité de l'information » au sein de la norme.

2.5.4. POINTS CONVERGENTS ENTRE LES CRITERES COMMUNS ET LA NORME ISO 27002

Nous retrouvons des préoccupations communes dans les deux normes comme, la protection des données de l'utilisateur, les termes de confidentialité, intégrité, disponibilité et traçabilité etc.

La norme ISO 27002 est ensemble de bonnes pratiques non techniques ou orientées produit telle que les critères communs CC/ISO 15408.

2.6. CONCLUSION

Ce chapitre a mis en lumière les possibilités de se protéger et les actions menées dans les organisations afin de sensibiliser les acteurs de celles-ci.

Nous allons aborder, dans le chapitre suivant les actions à mettre en œuvre et étudier des outils et méthodes pour sensibiliser les acteurs à la protection de l'information.

---

169 Source papyrus.bib.umontreal.ca

170 Source Wikipédia

CHAPITRE 3
SENSIBILISER A LA PROTECTION DE L'INFORMATION

« Au centre de la difficulté se trouve l'opportunité »
***Albert Einstein*[171].**

[171] Physicien et théoricien

3.1. INTRODUCTION

Nous aborderons, dans ce chapitre, plusieurs méthodes ou pistes à suivre, afin de mieux cerner les méthodes de transmission du savoir et comment aborder le public à sensibiliser.

3.2. L'APPROCHE COGNITIVE

3.2.1. LA DIDACTIQUE

La didactique nous pousse à nous poser les bonnes questions sur un objectif précis ; ici comment sensibiliser des acteurs de l'organisation.

Cette approche est différente de la pédagogie et, nous oblige à investiguer sur le fond de la transmission des savoirs, quels qu'ils soient.

➔ *DEFINITION*

> *« La didactique d'une discipline est la science qui étudie, pour un domaine particulier, les phénomènes d'enseignements, les conditions de la transmission de la « culture » propre à une institution et les conditions de l'acquisition des connaissances par un apprenant. » (Johsua et Dupin, 1989)*[172].

L'origine de la didactique se situe à l'antiquité, plus précisément aux temps des philosophes grecs et de la civilisation chinoise. L'adjectif « *didactique* » fait son apparition au Moyen Âge en 1554 (Grand dictionnaire Larousse). Le Robert (1955) et le Littré (1960) citent la didactique comme « *l'art d'enseigner* ».

➔ *OBJECTIF*

> *La didactique est une activité scientifique dont l'objet est l'étude de la construction des savoirs, identifiés, par des apprenants, qui construisent des connaissances, dans le cadre d'une institution ou d'un environnement de formation où, les apprenants interagissent avec des enseignants173.*

Des dispositifs informatisés peuvent être utilisés comme support à la formation

Le but de cette approche est de donner un sens à la transmission des savoirs (objectif commun), impliquer les acteurs afin, qu'ils soient moteur dans le changement.

➔ *DIFFERENCE ENTRE DIDACTIQUE ET PEDAGOGIE*

La didactique est une réflexion sur la transmission des savoirs.
La pédagogie est orientée vers les pratiques d'élèves en classe.

La didactique est centrée sur le contenu disciplinaire et les méthodes d'apprentissage. La pédagogie donne une méthodologie d'enseignement terrain avec des attitudes et, des actions à mener.

---

172 Source http://slideplayer.fr/slide/1619284/Bourgeois

173 Source Le système didactique Introduction à la didactique Karine Robinault – Master Didactiques et Interactions Octobre 2006

➔ *QU'ELLES SONT LES QUESTIONS SIMPLES A SE POSER POUR APPLIQUER LA DIDACTIQUE ?*

POURQUOI ENSEIGNER ?

Quels sont les objectifs de l'enseignement mené ? Pour répondre à cette question : la discipline, le niveau d'enseignement, le type de personnes concernées sont à considérer.

QUOI ENSEIGNER ?

Cette question concerne le contenu. Nous devons réfléchir aux attentes de notre public. Notre contenu correspondra aux besoins des personnels, de l'organisation autant au niveau personnel que professionnel.

À QUI ?

Qui est notre public ? Ce point est parfois difficile à mettre en œuvre au vu de la disparité des élèves (exemple à la Sorbonne, au collège…). Des tests d'évaluation peuvent être effectués afin de mieux cerner les apprenants.

L'enseignant sera formé à l'enseignement des adultes ou des enfants, afin de maîtriser le processus d'acquisition des savoirs et maîtriser le comportement psychologique à adopter, pour s'assurer de la transmission du savoir.

COMMENT ?

La pédagogie est en question : qu'elles sont les méthodes et les techniques misent en œuvre pour transmettre les savoirs. Chaque discipline à ses propres techniques.

COMMENT MESURER ?

Il faudra tester les résultats obtenus auprès du personnel concerné, les objectifs de départ, nos supports et nos méthodes d'enseignement.

PAR QUI ?

Il est évident que suivant l'enseignant et les méthodes qu'il emploiera le résultat sera différent. Ce sont des facteurs déterminants à prendre en considération.

3.2.2. METHODE D'APPRENTISSAGE COGNITIF

La méthode générale d'apprentissage cognitif, s'est différenciée de celle des pédagogues, en mettant en avant l'implication des apprenants et, des approches psychosociologues comme Abraham Maslow[174], Carl Rogers[175] ou Harold J. Leavitt[176].

Nous devons le développement de la Méthode d'Apprentissage Cognitif (*MAC*) – *Common Joke*

[174] Abraham Harold Maslow, né le 1er avril 1908 à New York et mort le 8 juin 1970 à Menlo Park en Californie, est un psychologue américain considéré comme le père de l'approche humaniste.

[175] Carl Ransom Rogers, né le 8 janvier 1902 à Oak Park (Illinois) et mort le 4 février 1987 à La Jolla (Californie), est un psychologue humaniste américain.

[176] Harold J. Leavitt (14 janvier 1922 - 8 décembre 2007) est un psychologue du travail et des organisations américaines

Broadcasting ou CJB — grâce aux travaux de recherche du psychologue Robert Mills Gagné[177] et, du sociologue français Edgar Morin[178].

La méthode d'apprentissage par l'expérience (*Experiential Learning/Outdoor Education*), née des recherches d'Alain Kerjean[179], un français, arriva en France en 1986. Cette méthode, déclinaison du courant cité ci-dessus, est un processus qui laisse la personne acquérir des compétences personnelles et sociales à partir d'expériences vécues et raisonnées.

Il s'agit d'une approche « *non formelle* » qui vient en complément de l'enseignement « *formel* ». Elle permet de développer des compétences qui, ne se transmettent pas par un enseignement traditionnel.

LA PSYCHOSOCIOLOGIE

Cette discipline a été fortement influencée par Abraham Maslow avec « *la hiérarchie des besoins et la théorie de la motivation* ».

Le discours de Carl Rogers[180] s'adresse aux enseignants et aux thérapeutes. Il explique qu'il « *faut avant tout se placer sur le même canal psychologique pour établir un véritable dialogue* », Carl Rogers, nomme cette attitude « *congruence* ».

ID n° 24 Pyramide des besoins de Maslow

L'apprenant sera regardé comme il est et non comme nous aimerions qu'il soit.

Cela sous-entend que nous ne prêterons pas nos propres sentiments à l'apprenant et nous éviterons toute projection.

Concrètement, **l'enseignant aura une attitude empathique**, ce qui implique d'être en adéquation avec l'apprenant. L'enseignant utilise les mots, les expressions et le langage de l'apprenant pour instaurer une proximité. Une confiance s'instaure, par rapport à cette attitude, et un dialogue se noue (attitude non-directive).

Cette méthode peut être complétée par un échange interactif : l'*Entretien semi directif*. Il s'agit d'une technique d'enquête, utilisée dans la recherche en science humaine, qui permet d'orienter la parole des personnes consultées, par rapport à un thème préalable défini.

---

177 Robert Mills Gagné (21 août 1916 - 28 avril 2002) est un psychologue américain.

178 Edgar Nahoum, dit Edgar Morin, né le 8 juillet 1921 à Paris, est un sociologue et philosophe français. « *Sept savoirs nécessaires à l'éducation du futur* »

179 Alain Kerjean est un écrivain et consultant français, né le 27 décembre 1951 à Paris. Il introduit en France en 1986 le courant pédagogique de l'apprentissage expérientiel (Experiential learning)

180 Carl Ransom Rogers, né le 8 janvier 1902 à Oak Park (Illinois) et mort le 4 février 1987 à La Jolla (Californie), est un psychologue humaniste américain. Il a principalement œuvré dans les champs de la psychologie clinique, de la psychothérapie, de la relation d'aide (counseling), de la médiation et de l'éducation.

3.2.3. PEI (PROGRAMME D'ENRICHISSEMENT INSTRUMENTAL)

Cette méthode est intéressante par son approche car, chaque individu est considéré pour ce qu'il est, avec son potentiel d'apprentissage.

Il nous semble judicieux d'extrapoler la méthode à une organisation. Les personnes que l'on rencontre ont un « *handicap de non-connaissance* » et sont démunies devant des situations de protection de l'information et d'attaques de criminels du net.

➔ *ORIGINE*

> *« Toute personne est capable de changement, quels que soient son âge, son handicap et la gravité de ce handicap. Les enfants différents ont simplement besoin d'un surcroît d'attention et d'investissement personnel » Reuven Feuerstein*[181]

Le PEI a été mis au point par le Professeur Feuerstein, dans les années cinquante pour les enfants issus de l'holocauste de la deuxième guerre mondiale. Les enfants étaient gravement atteints psychologiquement et dans l'incapacité à apprendre. De nos jours, le PEI est appliqué à des variétés de personnes comme des enfants en difficulté ou des adultes en formation continue et dans les entreprises.

Le développement de la structure cognitive des personnes est visé ici, elle est pratiquée en groupe (classe) ou individuellement.

Afin que ce blocage soit levé, une médiation humaine a lieu en analysant les expériences du « sujet » pour l'amener vers un but précis.

La théorie du changement et de l'apprentissage par médiation a abouti à deux pratiques :

- « *La méthode d'évaluation dynamique du potentiel d'apprentissage* »
- Le programme d'enrichissement instrumental (PEI).

➔ *OBJECTIF*

Le but du PEI, est de développer la réflexion chez une personne tout en corrigeant ses fonctions cognitives insuffisantes, de ce fait celle-ci pourra acquérir des connaissances plus facilement (voir Annexe n°1 page 179).

La valorisation de la personne est mise en avant en évitant toute mise en échec.

Tout d'abord il s'agit d'évaluer le « *potentiel d'apprentissage* » de la personne en lui faisant passer des tests, qui peuvent durer jusqu'à dix jours. Cette approche est contraire au test de QI qui nous positionne sur une échelle de grandeur en fonctionne des résultats obtenus.

Ici les tests sont adaptés à la personne qui est accompagnée dans leur réalisation par le médiateur.

La personne concernée (enfant ou adulte) passe les tests et le médiateur observe qu'elle est son approche par rapport à chaque question posée. Une correction est immédiatement opérée afin que le test se déroule correctement et aboutisse positivement. Le temps suivant est consacré à l'observation de l'apprentissage qui s'est opéré.

Le but de cet exercice est de comprendre ce que *« l'apprenant peut faire, et non de ce qu'il ne peut*

[181] Source https://3-bis.fr/quest-ce-que-la-methode-feuerstein/

pas faire ».

Le PEI se découpe en deux parties :

ENRICHISSEMENT

Il s'agit d'inculquer des stratégies d'apprentissage et de réflexion aux enfants ou adultes. Ce point a pour but d'enrichir l'esprit.

INSTRUMENTAL

Quatorze cahiers d'exercices ont été mis au point, afin de susciter les prérequis cognitifs qui font défaut à l'enfant ou à l'adulte. Chaque cahier est conçu pour répondre à dysfonctionnement cognitif précis. Le PEI est sans cesse revu et amélioré.

Le professeur a continué de s'occuper des enfants en difficultés, au sein de son institut bien après la fin de la guerre[182]. Cette méthode est depuis reconnue dans le monde entier[183].

3.2.4. ANDRAGOGIE, PEDAGOGIE ET HEUTAGOGIE

➔ *L'ANDRAGOGIE : SCIENCE D'ENSEIGNER AUX ADULTES*

ORIGINE

Le terme « andragogie » a été inventé par Alexander Kapp[184] en 1833 en Allemagne.

Ci-dessous le premier document utilisant le terme "Andragogie" : Kapp, Alexander (1833). Kapp, Alexander (1833) : *Platon's Erziehungslehre, als Paedagogik für die Einzelnen und als Staatspaedagogik. Minden und Leipzig*. (L'éducation de Platon, en tant que pédagogie pour l'individu et en tant qu'enseignement public. Minden et Leipzig).

Platon's
Erziehungslehre,
praktische Philosophie.
Dr. Alexander Kapp
1833

241
Dritter Theil.
Die Andragogik oder Bildung im männlichen Alter.
Nothwendigkeit der Weiterbildung im männlichen Alter.
§. 105.

ID n° 25 Le premier document utilisant le terme « Andragogie »

Ses premières réflexions ont été que l'apprentissage se fait par le biais de l'autoapprentissage et l'expérience de la vie, plutôt que par le seul fait de l'enseignement pur.

Cette approche de l'enseignement ou science anthropologique, guidera l'adulte vers la

182 « Le voyage d'Anton » de Mariana Loupan aux Presses de la Renaissance

183 4 852 enseignants ont été formés à cette discipline et 320 895 élèves en ont bénéficiés au Brésil (Bahia). Elle est enseignée à l'université PARIS XII dans le cadre de la formation : « Educabilité cognitive et Actes d'Apprentissages » par Christiane Montandon, maître de conférences.

184 Pédagogue allemand

connaissance et l'apprentissage des savoirs. Son étymologie est composée de deux mots de Grec ancien, *anèr*, *andros* (ἀνήρ, ἀνδρός), qui signifie « *l'homme* » et *agogos* (ἀγωγός), qui veut dire « *le guide* ». Le terme « *pédagogie* » signifie « *guider l'enfant* » et s'inspire de la philosophie de l'éducation qui la fonde.

Le mot d'andragogie, rebaptisé parfois « *anthropagogie* » apparait en Russie en 1855.

Cette méthode traverse l'atlantique jusqu'aux états Unis (Eduard C. Lindeman [185]en 1926) et a été mise en lumière par, Malcolm Shepherd Knowles[186], pionnier en matière d'éducation des adultes. Il est un précurseur du courant *humanisme contemporain*[187]qui prend en compte les aspects affectifs et cognitifs de l'individu pour favoriser son apprentissage, il place l'Homme au centre des dispositifs du savoir et de l'organisation social.

A contrario du *behaviorisme* (première moitié du XX siècle) qui prêche pour une réaction « réflexe » à la suite d'un stimulus d'un individu[188].

Malcolm Shepherd Knowles a commencé à élaborer une théorie sur l'andragogie pendant la Seconde Guerre mondiale après sa rencontre avec Dušan M. Savićević[189]. Son sujet thèse est la base de son premier ouvrage sur l'éducation des adultes, qu'il publia en 1950 sous le titre de *Informal Education Adult.*

Malcom Knowles a essayé d'introduire ses théories dans le reste de l'Europe en 1967, où il a reçu un accueil mitigé. Dès les années 1970, l'andragogie prend son essor et est reconnue comme d'autres disciplines académiques (médecine, biologie, physique etc.). L'université de Montréal reconnaît cette méthode en 1968-1969 et ouvre une voie de recherche sur l'enseignement des adultes en 1971-1972. L'andragogie est plus connue en l'Europe de l'est que dans le reste de l'Europe, ou la pédagogie est plus répandue.

PRINCIPES

L'andragogie désigne l'art et la science d'enseigner aux adultes. Elle s'oppose à la pédagogie, qui concerne l'enseignement des enfants.

Malcom Knowles bâti sa théorie autour de six principes :

- Le besoin : l'adulte a besoin de connaître la raison de l'apprentissage qu'il va commencer,
- Particularité : l'expérience de l'adulte (dont ses erreurs) est prise en compte,
- Investissement : l'adulte est impliqué dans l'organisation de l'apprentissage,
- Utilité : l'adulte souhaite apprendre des choses qui lui serviront concrètement à court terme, dans sa vie professionnelle et personnelle,

---

185 Eduard C. Lindeman (9/5885 – 13/4/1953) était un éducateur américain. Il a introduit de nombreux concepts d'éducation moderne des adultes dans son livre intitulé « The Meaning of Adult Education ».

186 Malcolm Shepherd Knowles (24/8/1913 à Livingston (Montana) – 27/11/1997) était un professeur américain.

187 « Quel « nouvel humanisme » francophone contemporain ? » Colloque international 16 au18 juin 2016 Université Paris-Sorbonne. Organisé par Centre International d'Études Francophones (CIEF), rattaché au Centre d'Études de la Langue et des Littératures Françaises (CELLF) de l'Université Paris-Sorbonne

188 Le béhaviorisme, behaviorisme ou comportementalisme est un paradigme de la psychologie scientifique selon lequel le comportement observable est essentiellement conditionné soit par les mécanismes de réponse réflexe à un stimulus donné, soit par l'histoire des interactions de l'individu avec son environnement, notamment les punitions et récompenses reçues par le passé (Wikipédia).

189 Enseignant à l'université de Belgrade à la faculté de philosophie.

- Modalité d'apprentissage : la mise en situation favorise l'apprentissage de l'adulte par rapport à une simple transmission des savoirs,
- Motivation : les adultes sont stimulés par une motivation intrinsèque[190].

> *« La motivation intrinsèque est une action conduite uniquement par l'intérêt et le plaisir que l'individu trouve à l'action, sans attente de récompense externe au contraire de la motivation extrinsèque qui est provoquée par une circonstance extérieure à l'individu (punition, récompense, pression sociale, obtention de l'approbation d'une personne tierce) ».*[191]

- La méthode extrinsèque est un des fondements du béhaviorisme.

L'adulte adhéra à un enseignement que si la formation à un sens

LE ROLE DU FORMATEUR D'ADULTES

Une mise en situation favorisant l'apprentissage sera organisée par le formateur tout en mettant en valeur les savoirs détenus dans le groupe, c'est pourquoi le formateur est qualifié de « *facilitateur* » ou de « *médiateur* ».

Le formateur fera la liaison entre l'apprenant et un contenu (des savoirs, des savoir-faire, des savoirs être) et les relations dans le groupe.

➔ *LA PEDAGOGIE : L'ENSEIGNEMENT DES ENFANTS*

ORIGINE

Le pédagogue (« *paidagogos* »), dans la Grèce antique désignait un esclave et aussi le fait, pour une personne, de choisir des disciplines et le précepteur qui les lui enseigneraient. Le rôle du pédagogue est la médiation entre un enfant et le savoir.

Aujourd'hui le terme s'est élargi et comprend les principes et les méthodes qui favorisent l'apprentissage. La pédagogie s'appuie sur d'autres disciplines comme la psychologie, la sociologie, la linguistique, l'anthropologie, la philosophie ou la médecine.

PRINCIPES

La pédagogie concerne l'enseignement des enfants par opposition à l'andragogie qui est « l'art et la science d'enseigner aux adultes ».

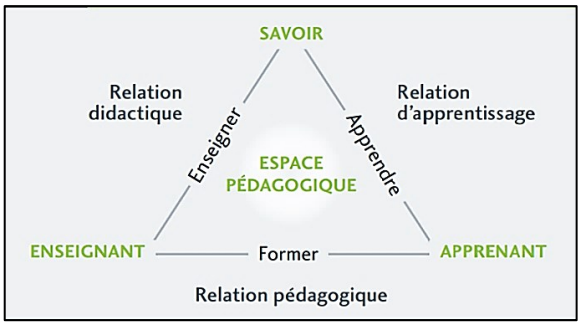
Nous pouvons situer l'acte pédagogique dans un « *triangle pédagogique* »[192] :

---

190 Théorie de Richard Deci en 1975 et enrichie par Deci et Ryan (1985, 2002). Source http://alain.battandier.free.fr/spip.php?article19.

191 Source http://alain.battandier.free.fr/

192 Ses trois côtés représentent ce que Jean Houssaye appelle un « processus », soit la relation entre deux des trois pôles : le savoir, le professeur, les élèves.



ID n° 26 « triangle pédagogique » de Jean Houssaye[193]

C'est un triangle pédagogique qui met en relation les 3 processus suivants :

- Enseigner (relation entre l'enseignant et le savoir),
- Former (relation entre les enseignants et les élèves),
- Apprendre (relation entre les élèves et le savoir).

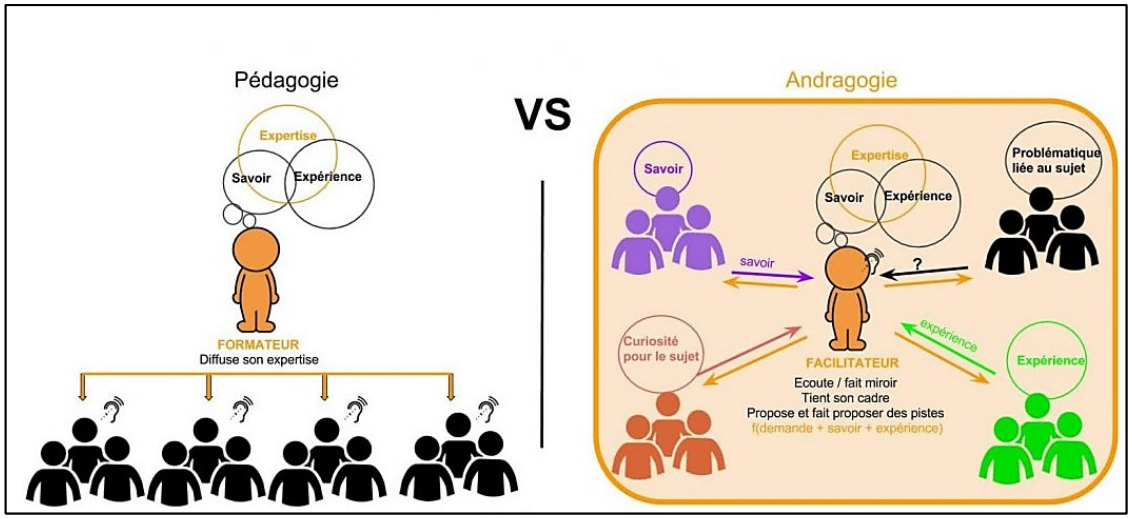
DIFFERENCE ENTRE LA PEDAGOGIE ET L'ANDRAGOGIE

L'ENFANT	L'ADULTE
Apprend pour plus tard,	Apprend pour maintenant,
Participe sur une base obligatoire,	Participe sur une base volontaire,
Poursuit des objectifs fixés par d'autres (motivation d'autrui),	Poursuit des objectifs personnels (motivation personnelle),
Comble un besoin d'acquisition des connaissances,	Adapte et complète sans cesse ses connaissances,
Possède une expérience limitée et peu intégrée,	Possède une expérience complète, diversifiée et très intégrée,
S'interroge à l'occasion sur l'utilité de ce qu'on lui enseigne,	Démontre une volonté systématique de percevoir cette utilité,
Manifeste peu d'intérêt d'apprendre des autres membres d'un groupe d'élèves,	Manifeste de l'intérêt à écouter et à partager les connaissances et les expériences des différents membres d'un groupe d'apprenants,
Perçoit le temps comme étant une ressource illimitée (l'enfant a tout son temps),	A une conscience aiguë de la valeur du temps (le temps c'est de l'argent),
Démontre une ouverture à apprendre un grand nombre de choses différentes,	A des intérêts plus restreints liés aux difficultés qu'il rencontre,
A une prise en charge limitée de son propre apprentissage,	Cherche à augmenter la prise en charge de son propre apprentissage,
S'adapte facilement à la nouveauté,	S'adapte plus difficilement à la nouveauté,
Possède une capacité physique et de concentration sur une plus longue période, ce qui facilite l'apprentissage.	Possède une capacité physique et de concentration moins grande, ce qui peut rendre l'apprentissage plus difficile.

Figure 1 Source : Tableau adapté de S. Pouliot (1997), « Éducation pour la santé : recueil de textes », inédit, Université de Laval, UQAR et UQTR.

Ce tableau peut être schématisé sous la forme suivante :

[193] Jean Houssaye, Le triangle pédagogique. Théorie et pratiques de l'éducation scolaire, Peter Lang, Berne, 2000 (3e Édition 1re Éd. 1988)



ID n° 27 Différence entre pédagogie et andragogie. Source de l'image colimaez.bzh

Un adulte (apprenant) est motivé pour suivre une formation (en lien avec son expérience) contrairement à un enfant, qui sera plus passif devant l'enseignement reçu.

Le formateur exprimera clairement les objectifs à atteindre à la fin de la formation car l'apprenant veut comprendre l'utilité de l'enseignement et comment le mettre en œuvre de retour dans son milieu professionnel. Il est fréquent dans les formations, d'entendre les apprenants demander des exemples concrets au formateur, ce phénomène s'est vérifié lors de la formation du master.

Nous devons prendre soin de créer une ambiance propice à l'échange et favoriser une synergie dans le groupe et de gagner la confiance des apprenants.

A l'inverse la pédagogie est un enseignement « descendant », le formateur dispense sa connaissance et l'apprenant intègre, ou pas, les préceptes.

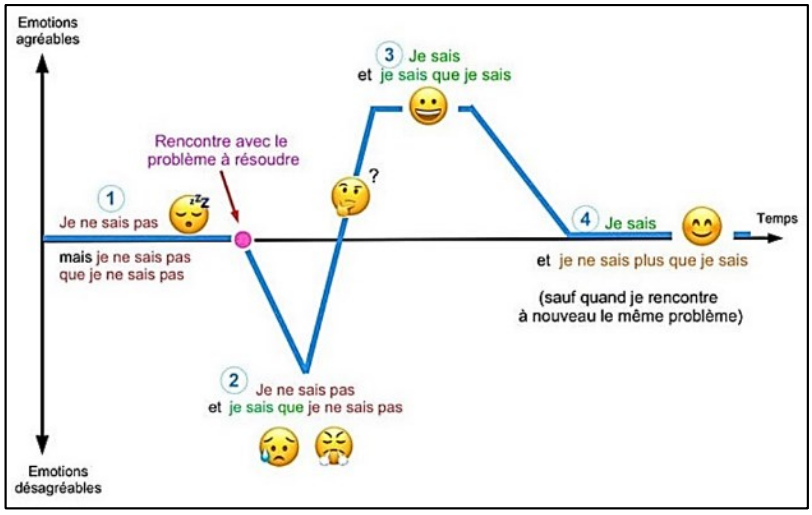
Le formateur tiendra compte de l'hétérogénéité du groupe afin d'adapter son enseignement. Ce point est régulièrement reproché à la pédagogie, car l'éducation nationale dispense en enseignement uniforme sans tenir compte de la particularité des enfants. Des mouvements d'enseignement alternatifs, comme Montessori, sont nés de cet état de fait.

Donc le formateur à la différence de l'enseignant s'inscrira dans une relation entre adultes et favorisera la synergie de groupe, se basant sur des faits. Celui-ci ne devra pas s'offusquer d'être contredit, car l'apprenant peut être critique si celui-ci pense que le savoir dispensé est contradictoire avec son expérience.

➔ *L'HEUTAGOGIE : APPRENDRE A APPRENDRE !*

L'heutagogie est l'autoapprentissage, c'est une manière de donner les moyens aux hommes de tout âge à apprendre par eux-mêmes, c'est le troisième volet complémentaire de l'andragogie et la pédagogie.

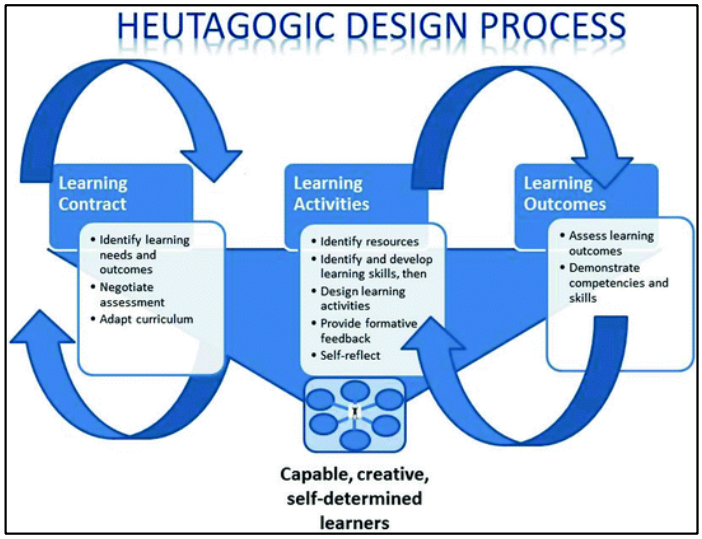
Cette méthode permet aux apprenants d'acquérir des compétences et des capacités. Les compétences sont, la mise œuvre d'apprentissage, dans un contexte particulier (personnel ou professionnel) de façon appropriée. Les capacités se traduisent par la confiance qu'à l'apprenant en ses compétences et son aptitude à prendre la bonne décision, au bon moment pour résoudre un problème.



ID n° 28 cycle "apprendre à apprendre"

Trois principes doivent être respectés : défi, autonomie et support :

- L'enseignant déterminera avec l'apprenant ce qu'il souhaite apprendre et comment ses connaissances seront évaluées (défi).
- Ce schéma s'applique tout à fait à la formation en ligne, par exemple, en matière de sensibilisation à la protection de l'information (autonomie, média utilisé).
- L'enseignant se situe à côté de l'apprenant pour l'encourager dans son parcours, l'éclairer sur ses difficultés et lui apporter un support.



ID n° 29 principe de l'heutagogie. Source https://www.skillogs.com/heutagogie/

➔ *OUTILS*

Des outils ludiques peuvent être employés pour tester l'apprentissage ou le provoquer (voir Annexe n°14 page 189) :

- Organiser un questionnaire géant, à la fin d'une campagne de sensibilisation (exemple : https://kahoot.com/, https://quizizz.com/, https://www.plickers.com/),
- Mettre en place des jeux de rôle (http://pedagopsy.eu/jeu_de_role.html). L'avantage des jeux de rôles est qu'ils permettent d'articuler la théorie acquise lors de l'apprentissage et la

pratique sur le terrain. Le jeu de rôles constitue un support d'exercices structuré ayant pour objectif la formation des acteurs de l'organisation et non un divertissement.[194].

- Demander à une troupe de théâtre amateurs de jouer des saynètes réalistes, comme un trajet en train avec un ordinateur portable et le voisin qui regarde l'écran alors que vous traitez un document confidentiel (exemple : https://youtu.be/ueM96Cl5Y5I)
- Mettre en place un « escape game » : un groupe de personnes est enfermé et doit trouver des indices et résoudre des énigmes pour sortir d'un local (exemple : cas d'ingénierie social, ou comme à la recherche du pirate informatique, etc.)
- Le jeu des 7 erreurs à la mode Cluedo (exemple : documents confidentiels laissés sur une imprimante, clef USB tombé sur le sol dans un couloir, etc.).
- Passer le permis de bonne conduite sur internet (exemple : http://www.passe-ton-permis-web.com/). Le permis est obtenu après avoir répondu à 10 questions sur des situations rencontrées fréquemment sur Internet.

D'autres outils numériques sont disponibles pour réaliser des questionnaires : https://dane.ac-lyon.fr/spip/Comparatif-des-outils-numeriques#, https://moodle.org/, http://numeriques.spip.ac-rouen.fr/?lang=fr,

- Enrôler les acteurs dans des MOOC (exemple : Soyez acteur de la sécurité de l'information chez https://www.fun-mooc.fr/courses/unormandie/68001S02/session02/about).
- Etc…

[194] Le jeu de rôles : pratique de formation pour un public d'adultes par Bertille Patin Université de Haute-Bretagne, Rennes 2

➔ *COMPARAISON DES TROIS APPROCHES*

	Pédagogie Apprentissage chez l'enfant	Andragogie Apprentissage chez l'adulte	Heutagogie Apprentissage auto-dirigé
Dépendance	L'apprenant est une personne dépendante. L'enseignant définit le contenu, la méthode et la temporalité des apprentissages.	L'apprenant est indépendant, il évolue vers l'autonomie et l'indépendance dans ses apprentissages.	Les apprenants sont interdépendants. Ils se questionnent réguilièrement sur les opportunités d'apprentissage à travers les expériences vécues.
Ressources mobilisées	L'apprenant a peu de ressources. L'enseignant élabore des techniques de transmissions pour aider l'apprenant à mémoriser.	Les adultes s'appuient sur l'expérience (la leur ou celle des autres)	L'enseignant propose des ressources mais les apprenants choisissent leur propre chemin, selon l'objectif visé.
Raisons pour apprendre	Apprendre pour avancer jusqu'à l'étape suivante	Les adultes apprennent quand ils ressentent le besoin de savoir ou d'être plus efficace.	L'apprentissage n'est ni planifié, ni linéaire. Il ne répond pas à un besoin mais est suscité par une opportunité à saisir.
Focus de l'apprentissage	L'apprentissage est centré sur le contenu, organisé autour d'un curriculum prescit et un enchaînement logique des séquences	L'apprentissage des adultes est centré sur un tâche ou un problème à résoudre.	Les apprenants vont au-delà de la résolution de problèmes en étant pro-actifs. Ils s'appuient sur l'expérience, l'analyse réflexive et les interactions avec leur
Motivations	La motivation vient de sources externes : le plus souvent des parents, des enseignants et d'un esprit de compétition	Les sources de motivation sont internes : estime de soi, confiance et reconnaissance, qui découlent d'une réalisation.	Capacité à exploiter ses compétences : efficacité personnelle, apprendre à apprendre, créativité, collaboration.
Rôle du formateur / enseignant	Il conçoit le processus d'apprentissage, impose le matériel. Il détient le savoir.	Animateur ou facilitateur, il crée un climat de collaboration, de respect et d'ouverture.	Il aide l'apprenant à développer ses capacités. Il sait apprendre à apprendre, travailler à plusieurs et est créatif. Il utilise ses compétences dans toutes les situations et à un bon sens de l'auto-efficacité.

traduction de http://www.blog.lindymckeown.com/?p=52 Jackdub

ID n° 30 Comparaison des trois approches : pédagogie, andragogie et heutagogie

L'andragogie et l'heutagogie sont complémentaires ; la deuxième vient en appuis de la première et en fait partie à part entière.

3.3. LA CONDUITE DU CHANGEMENT

3.3.1. DESIGN THINKING

Le Design Thinking est centré sur l'homme

Le Design Thinking est né dans les années 1950 avec une nouvelle approche de l'animation des réunions par Alex Osborn (publicitaire américain). Un programme a été mis en place et développé à Stanford dans les années soixante par Rolf Faste[195] à partir des travaux de Robert McKim[196].

Le premier ouvrage « Design Thinking » est publié en 1987 aux presses du MIT par Peter Rowe. Le design thinking évolue avec la création de l'agence de David Kelley[197] à Palo Alto,

« Penser comme un designer peut transformer la façon dont vous développez des produits, des services et processus et même des stratégies ».
Tim Brown, président d'IDEO.[198]

L'expérience est au centre du concept provoquant l'engagement fort des acteurs concernés.

Les concepts sont visualisés, et ne sont plus expliqués avec des mots. Il est prouvé que le visuel est interprété 60 000 fois plus rapidement par notre cerveau que le texte[199], ce concept est à appliquer dans l'usage des supports de sensibilisation.

Moins de texte... Et plus d'images

Le Design Thinking peut être synthétisé en trois parties :

- Identifier une problématique et comprendre son environnement (« empathy » et « define »),
- Trouver une idée, un concept qui permettra de résoudre cette problématique (« ideate »)
- Concevoir la forme qui incarnera le concept (« prototype » et « test »)

Le concept se rapproche de la roue de Deming, il s'agit d'un cycle représenté sous forme d'une lemniscate (courbe plane ayant la forme d'un 8) :

---

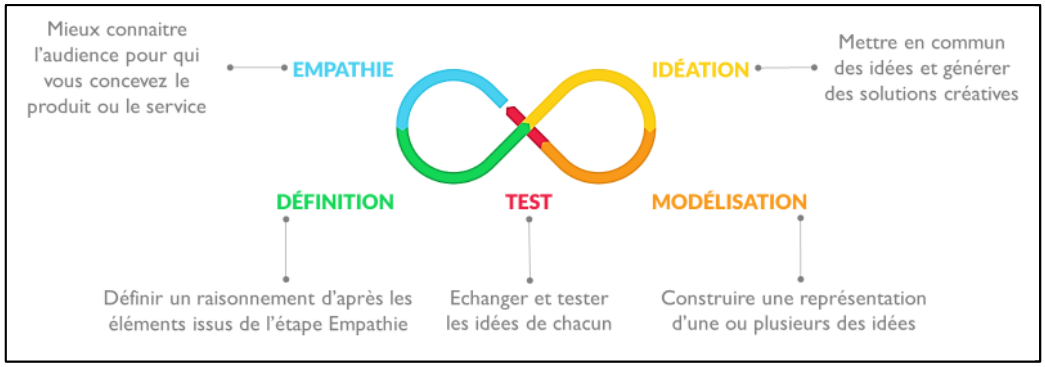
195 Rolf A. Faste (1943-2003) était un designer américain directeur du Stanford Joint Program in Design de 1984 à 2003. Il est connu pour ses contributions à la pratique du design créatif, ou «design thinking », qu'il a été le pionnier de l'approche de la « personne dans son ensemble » pour la résolution de problèmes centrée sur la perception du besoin.

196 McKim, Robert H., Experiences in visual thinking, Monterey (U.S.A), Brooks/Cole, 1972, 171 p

197 Fondateur de la société de design IDEO, enseignant à Stanford dès 1990. Biographie : https://www.ideo.com/people/david-kelley

198 Source https://www.ideo.com/about. IDEO est l'entreprise qui a le plus contribué à la popularisation du concept,

199 Source 3M Corporation : http://www.billiondollargraphics.com/infographics.html voir infographie à https://www.redacteur.com/blog/wp-content/uploads/2017/11/cerveau-traite-contenu-web.jpg



ID n° 31 Design thinking, a framework or innovation adapté du concept de. Billy Loizou

Nous devons faire abstraction de pensées systématiques, préalablement définies et se placer à un niveau inhabituel dans le cadre de la sensibilisation.

Rester centré sur l'humain

L'empathie envers les acteurs de l'organisation mènera le jeu afin, de créer un impact positif sur les relations entre les personnes, la démarche, l'organisation et l'interaction au sein des groupes.

L'acteur rentre dans le jeu et s'imprègne de la protection de l'information, participe, créé des concepts, des slogans, partage ses craintes et ses besoins. L'acteur est ici considéré comme le « client » dans le concept du Design Thinking et le responsable de la sensibilisation comme « l'entreprise » ou le service marketing de l'organisation.

Le résultat des ateliers de sensibilisation, et/ou de travail, permettra de mettre en œuvre des campagnes de sensibilisation qui toucheront « *vraiment* » les différents acteurs de l'organisation et de répondre aux besoins de sécurisation. Les différentes parties prenantes, pourront échanger et comprendre les contraintes réciproques afin d'apporter des solutions avec un certain consensus.

Nous pouvons nous appuyer sur le mimétisme comportemental ou un effet boule de neige : le groupe sensibilisé influencera leurs collègues, prestataires, fournisseurs, etc.

Les acteurs de l'organisation seront sectorisés afin de les sensibiliser sur des sujets communs et aussi (voir §Sectoriser des acteurs à sensibiliser page 106) mélangés, afin que la rencontre soit enrichissante et que des problématiques diverses ressortent. Cet exercice permettra à la personne en charge de la sensibilisation, de relever des problèmes et aussi de renforcer la cohésion d'un groupe autour d'un sujet commun qui regarde au plus haut point l'organisation.

Roger Martin de l'Université de Toronto [200] présente le « Design Thinking » comme « *se situant au carrefour de la pensée analytique (preuve chiffrée) et de la pensée intuitive (savoir sans raisonnement préalable)* ».

[200] Roger Martin a été doyen de la Rotman School de 1998 à 2013 et a fait des recherches sur la pensée intégrative, le design d'entreprise et la compétitivité des pays. http://rogerlmartin.com/. "*the design of business, why design thinking is the next competitive advantage*" Harvard Business Review Press; Third Edition (October 13, 2009)

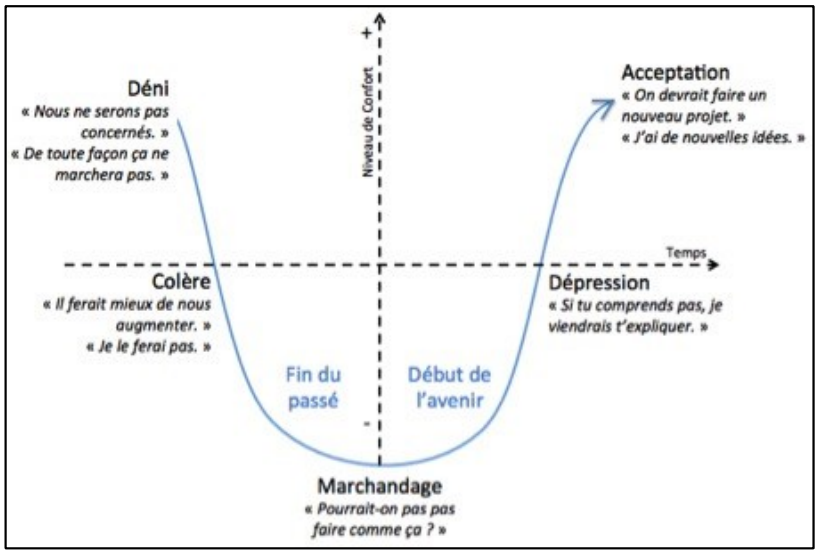
3.3.2. ADKAR - DCMDA

La méthode *ADKAR*, a été inventée en 1981 par la société américaine *Prosci*[201], basée dans le Colorado. Des recherches effectuées, pendant 14 ans, avec plus de 2 600 entreprises, ayant opéré des changements profonds, ont donné naissance à un outil de conduite au changement nommé *ADKAR*. Depuis 1998, tous les deux ans, Prosci publie les résultats de son étude des changements dans les organisations.

Ce modèle est complémentaire à celui de Kübler Ross[202] car il force à réfléchir sur les actions à entreprendre pour piloter le changement et le rendre pérenne.

Kübler Ross a focalisé ses études sur la fin de vie et les soins palliatifs apportés aux personnes. Elle formalisa le cheminement émotionnel auquel une personne est soumise lorsqu'elle apprend qu'elle va bientôt mourir.

Sa théorie a été popularisée et qualifie maintenant les étapes par lesquelles passe une personne lorsqu'elle change de paradigme.



ID n° 32 Modèle de Kübler Ross appliqué au changement

Le succès de notre démarche, dépend de ce qu'un grand nombre d'acteurs de l'organisation changent, leur façon d'agir vis-à-vis de la protection de l'information. Réussir à convaincre des personnes de bonne volonté ne suffit pas, comme le démontre le modèle *ADKAR*.

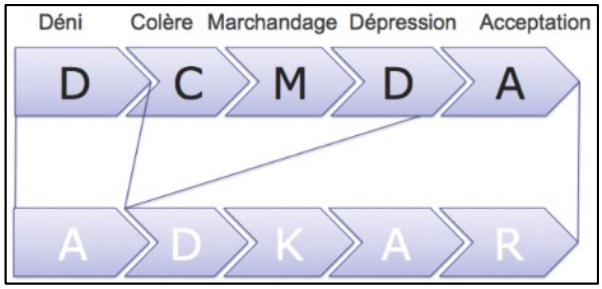
ADKAR peut être utilisé pour :

- Diagnostiquer la résistance au changement,
- Aider le personnel dans les phases transitoires,
- Créer un plan d'actions efficace pour obtenir des changements.

Du modèle de Kübler Ross on associe des actions du modèle ADKAR :

201 https://www.prosci.com/

202 Elisabeth Kübler-Ross (1926-2004) était une psychiatre et psychologue helvético-américaine.



ID n° 33 Modèle ADKAR

À chaque lettre du modèle correspond une étape :

QUESTIONS	QUI	CONSIDERATION
Awareness / Conscience Première étape, Faire savoir que l'on va changer et les actions à mener		
Pourquoi je devrais changer quoi que ce soit à ce que je fais, je ne sais pas.	C'est le commanditaire qui prendra la parole et exprimera au plus grand nombre les quatre points suivants (l'Awareness, ou prise de conscience).	Qu'est-ce qui a besoin de changer ? Pourquoi changer ? Qu'est-ce qu'on risque si on n'arrive pas à changer ? En quoi changer nous permet d'atteindre nos objectifs business ?
Desire / Désir Le Désir est ce qui fait que j'ai à titre personnel, envie de changer. Ces raisons sont de plusieurs natures : Technique, Politique, Culturel ou Individuel et sont propres à chaque individu.		
En quoi ça me concerne, ce n'est pas clair, ce que j'y gagne, non plus.	C'est le manageur de proximité qui prendra la parole et clarifiera avec son collaborateur, dans un entretien seul à seul (la conversation Desire)	Ce qui change dans les activités du collaborateur Les nouvelles responsabilités Ce que le collaborateur y gagne personnellement Et ce que l'équipe y gagne collectivement
Knowledge / Connaissance Ce sont les savoirs et les compétences qu'il va falloir acquérir, à titre individuel, pour continuer à bien faire mon métier une fois le changement effectué.		
Comment ça marche et comment je peux m'y adapter, je l'ignore.	Le formateur est la personne-ressource pour combler cette fosse, bien sûr. Il utilise enseignement, évocations, explications et exercices. Il utilise les sujets quotidiens des participants. Au passage, nul besoin que le formateur diffuse lui aussi les messages du commanditaire : il n'est pas légitime pour cela, et ça décrédibiliserait peut-être le message lui-même.	
Ability / Maîtrise pratique / Aptitude Les cadres et leaders doivent pleinement jouer leurs rôles si l'on veut que le changement prenne et surtout soit pérenne. Il s'agit de pouvoir évaluer la situation pour entreprendre le changement à titre individuel ou groupe de plusieurs personnes.		
Comment résoudre les nouveaux problèmes du quotidien, je sèche.	Le manageur de proximité est la clé du succès comme à la suite de la formation.	Encourager le collaborateur désorienté, écouter ses récriminations, Demander son effort, Accompagner ses progrès,

QUESTIONS	QUI	CONSIDERATION
		Proposer des solutions, etc.
Renforcement / Renforcement Ce sont toutes les actions qui vont permettre de rendre pérenne le changement.		
Est-ce que tout ça a servi à quelque chose, j'en doute.	C'est le commanditaire qui reprendra la parole et renforcera le changement	Evaluer ce qui a été fait, Confirmer ce qui fonctionne, Clarifier ce qui reste à accomplir, Utiliser les mots magiques de la relation : merci, s'il vous plaît, pardon, courage, bravo.

ID n° 34Modèle ADKAR

La conduite de changement est menée, étape par étape, après validation par le commanditaire. On découpe les tâches en actions gérables, que l'on peut réellement réaliser, réussir et terminer avec les acteurs de l'organisation.

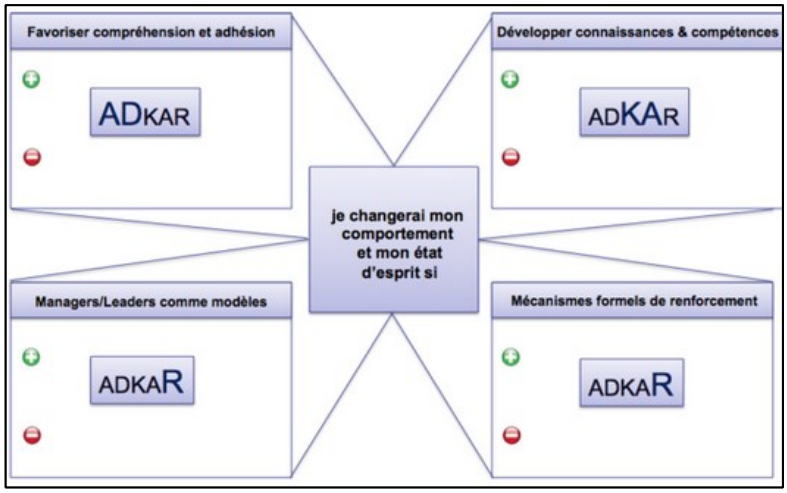
Le premier point est la découverte de l'environnement de l'organisation, les acteurs de l'entreprise, identifier le commanditaire (la Direction ?), préparer des messages clairs, converser avec les parties prenantes. Ces actions prennent du temps, mais la réussite sera présente si la préparation terrain est méthodique.

Préparer et converser pour réussir vite et pour longtemps.
Plutôt tortue que lièvre.

Le modèle *ADKAR* nivelle le terrain, le rôle de chacun est clair : le commanditaire est la conscience et renforce la démarche par son statut, les manageurs motivent et coachent, les formateurs forment et les collaborateurs adhèrent au changement !

La personne en charge de mener la conduite du changement, c'est-à-dire comment utiliser des bonnes pratiques de la protection de l'information, n'est pas seule pour faire adhérer les acteurs au changement. Il s'appuiera sur le commanditaire, les cadres, les formateurs et les acteurs de l'organisation.

Nous pouvons utiliser « *la matrice* d'influence », ci-dessous, qui permet, de positionner de façon structurée, les actions identifiées par l'approche *ADKAR*. Pour chaque « *secteur* », nous allons noter les + et les - que nous avons, ce qui nous permettra plus facilement d'en déduire les actions correctives.



ID n° 35 la matrice d'influence ADKAR

Pascal Le Deley [203]propose une feuille de route fondée sur la méthode *ADKAR*, qui à l'origine se présente de manière globale :

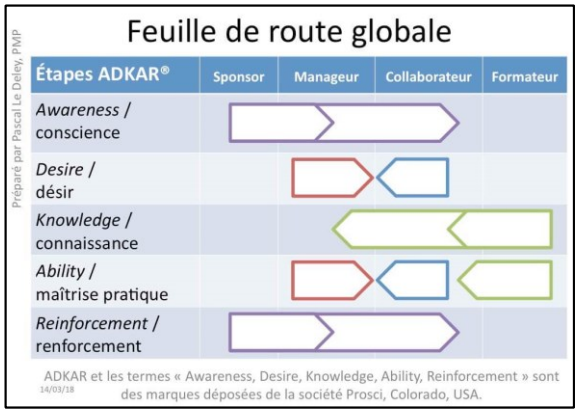
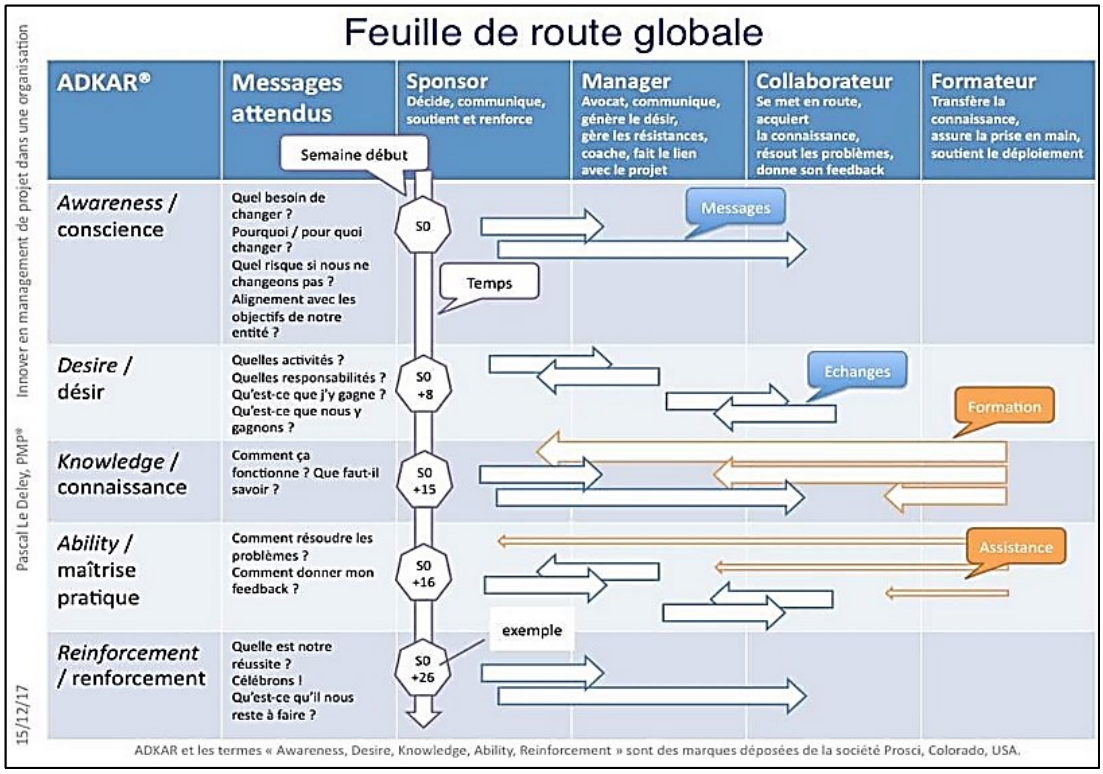


Figure 2 Feuille de route globale de la méthode ADKAR



ID n° 36 Feuille de route de mise en œuvre de la méthode ADKAR par Pascal Le Deley

Cette feuille route est vue comme un projet. Les étapes sont fractionnées afin de permettre des échanges entre les différents acteurs, après validation du commanditaire (sponsor), nous découpons les tâches par des actions gérables.

Le deuxième aspect positif est de proposer des étapes rapides à traiter, c'est encourageant pour les acteurs et cela ménage leur agenda !

[203] Pascal Le Deley est professionnel du management de projet, certifié PMP et intervient dans les grands groupes en utilisant le modèle ADKAR http://projet-initiative101.com/biographie/

3.3.3. L'EQUATION DU CHANGEMENT

Nous souhaitons changer les habitudes des acteurs de l'organisation !
C'est bien, mais notre seule volonté ne suffit pas !

La sécurisation des informations oblige les organisations à modifier leur vision et leur processus.

Le terme de conduite de changement ou d'accompagnement est employé lors de la mise en place d'un projet, mais on ne sait pas vraiment ce que cela implique.

Plusieurs ingrédients doivent être présents pour que notre démarche aboutisse et se pérennise :

VISION	+	COMPETENCES	+	MOTIVATION	+	RESSOURCE	+	PLAN D'ACTIONS	=	CHANGEMENT
	+	COMPETENCES	+	MOTIVATION	+	RESSOURCE	+	PLAN D'ACTIONS	=	CONFUSION
VISION	+		+	MOTIVATION	+	RESSOURCE	+	PLAN D'ACTIONS	=	ANXIETE
VISION	+	COMPETENCES	+		+	RESSOURCE	+	PLAN D'ACTIONS	=	CHANGEMENT PROGRESSIF
VISION	+	COMPETENCES	+	MOTIVATION	+		+	PLAN D'ACTIONS	=	FRUSTRATION
VISION	+	COMPETENCES	+	MOTIVATION	+	RESSOURCE	+		=	FAUX DEPART

ID n° 37 l'équation du changement source https://wikilean.com/articles-lean-six-sigma-management-conduire-changement-conduite-changement/

- *VISION* : la vision exprimera clairement par le responsable du changement. Un but imprécis entraînera une vision confuse. Les parties prenantes du projet ne sauront pas comment aller dans la bonne direction.
- *COMPETENCES* : les acteurs du projet vont se demander comment mener à bien les actions demandées dans le cadre du projet. Un accompagnement sera nécessaire pour les rassurer et leur permettre d'atteindre les buts que nous nous sommes fixés.
- *MOTIVATION* : la motivation des acteurs du changement, seule est insuffisante.
- *RESSOURCES* : le manque de ressource suffisante à la conduite du projet ne permettra pas son aboutissement. Cette situation sera frustrante pour les personnes impliquées, même si elles sont motivées.
- *PLAN D'ACTION* : le plan d'action sera clair, précis et concret. Dans le cas contraire cela sera l'anarchie et projet avortera.

L'ensemble des points, du tableau ci-dessus, doivent être présents dans la mise en œuvre du projet pour assurer sa réussite.

3.3.4. GENBA WALK

Genba walk, parfois écrit gemba, est d'origine japonaise et signifie « *là où se trouve la réalité* », c'est-à-dire sur le terrain.

Ce terme est repris en lean management[204] pour signifier : « *terrain* », « *atelier* », ou « *poste de travail* ». Toujours dans ce domaine, le terme connexe Genba walk désigne l'action d'aller voir le processus réel, de comprendre le travail, de poser des questions et d'apprendre sur place. Par extrapolation, le Genba walk concerne tous les lieux où se crée de la valeur (exemple : qualité d'un produit ou d'un service).

Le Genba walk n'est pas le lieu pour résoudre les problèmes,
C'est le lieu pour les comprendre et les partager.

[204] Méthode de gestion de la production qui se concentre sur la « gestion sans gaspillage »

Le président de Toyota, Fujio Cho, résume la démarche ainsi : « *aller voir, demander pourquoi, montrer son respect (Go see, ask why, show respect)* ».

Comment prétendre être pertinent sans savoir de quoi on parle ?

La démarche de la sécurisation de l'information s'inscrit tout à fait avec cette approche. Il est nécessaire de se rendre sur le terrain pour :

- Instaurer une relation de confiance et montrer de l'intéressement à l'activité des acteurs de l'organisation,
- Comprendre le métier des acteurs de l'organisation,
- Comprendre leurs besoins et leur problématique quotidienne,
- Cerner l'écosystème dans lequel les acteurs de l'organisation évoluent (présence de public, stress)
- Comprendre les flux et les interactions entre les personnes, les applications, les processus, etc.
- Commencer la conduite de changement,

Les acteurs maîtrisent leur milieu, leur métier et sont plus à l'aise dans leur environnement pour parler.

Les explications données seront plus claires et la démarche productive, en face-à-face, avec un utilisateur qui, en plus de l'explication verbale, pourra montrer visuellement à quoi il est exposé. Cela permettra de gagner du temps dans la récolte des risques.

Au lieu de provoquer des réunions interminables et improductives, pourquoi ne pas se rendre sur le terrain ?

Le Genba Walk peut être comparé à un audit, et il se préparera comme tel. Les premières visites sur le terrain seront guidées par un fil rouge sur lequel on focalisera son attention.

Dans un premier temps, on peut se concentrer sur une zone, un groupe de travail, un service et regarder les acteurs travailler. L'objectif est de comprendre ce qu'il se passe et de relever les dysfonctionnements.

L'esprit restera ouvert durant l'observation. Des facteurs multiples peuvent provoquer des perturbations, auxquelles les personnels répondent au mieux. En aucun cas il s'agit de stigmatiser les employés, à quelque niveau que ce soit ; cette réaction anéantirait toute la démarche par la perte de confiance et la cassure de la relation que nous tentons d'établir.

Les dysfonctionnements collectés permettront d'alimenter une campagne de sensibilisation, d'apporter les réponses et des moyens pour sécuriser l'information. Les bonnes pratiques seront couplées à des exemples concrets.

Nous développerons plus loin le cas du patient traceur, qui est un dérivé du Genba Walk ou le parcours des nouveaux arrivés. Cette méthode peut également s'appliquer à tout type de parcours comme une visite d'entreprise par un client pendant laquelle nous relèverons toute information sensible à laquelle il pourrait avoir accès (équipements spécifiques, capacités de production, laboratoires…) ou se promener dans l'entreprise et relever toute information confidentielle à portée de vue (bureau, mur, chevalet de conférence, salle de réunion, écran d'ordinateur…).

ID n° 38 les dix questions à poser source de l'image https://jpdconseil.com/

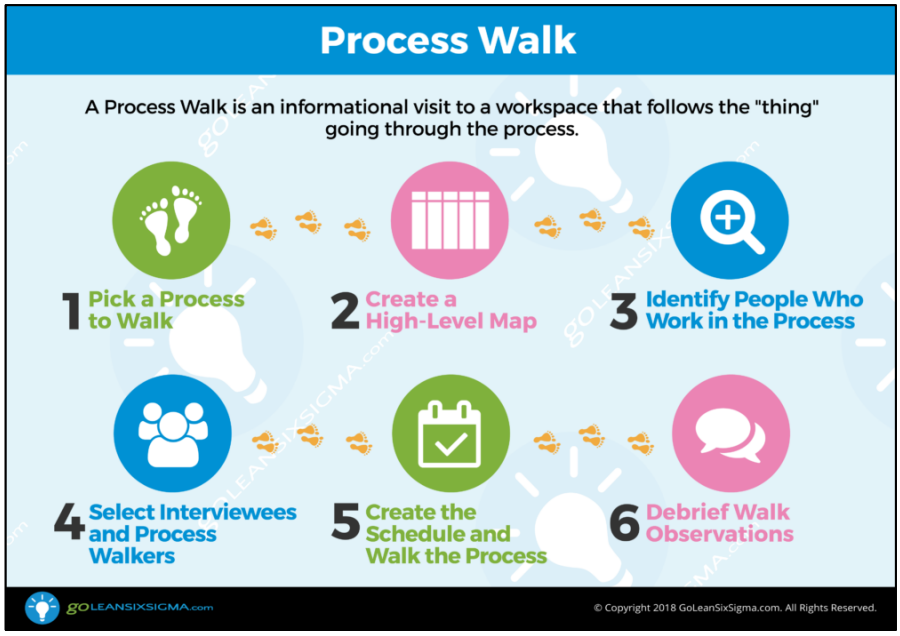


Figure 3 Processus du Genba Walk source de l'image https://goleansixsigma.com/

Le processus est jalonné d'entretiens structurés sur le terrain avec des participants représentatifs du processus, dans le but d'obtenir une compréhension globale du processus. Les entretiens portent sur des détails tels que le temps de traitement, le temps d'attente, les taux de défauts, les causes profondes et d'autres informations pouvant conduire à des améliorations ciblées.

➔ *COMPARAISON AVEC LE PATIENT TRACEUR*

Le patient traceur, mis en place par la Haute Autorité en Santé, lors des certifications est une approche Genba Walk. La méthode du patient traceur permet d'analyser le parcours d'un patient de l'amont jusqu'à l'aval de son séjour à l'hôpital en tenant compte des processus de soins et de l'ensemble des organisations nécessaires à la prise en charge.

La méthode est issue de l'expérience de la *Joint Commission* aux Etats-Unis (Joint Commission

2008[205]) et a été adaptée en France à l'occasion de la certification des établissements de santé.

Elle permet de révéler d'éventuels dysfonctionnements qui contribuent, à élaborer un diagnostic fondé sur des approches croisées (audit de processus, autres méthodes d'évaluation des pratiques professionnelles EPP), mais elle n'est pas une méthode statistique.

Les professionnels sont satisfaits par cette méthode et trouvent la démarche motivante et concrète. Elle donne une vision globale de la prise en charge d'un patient et, permet de découvrir des éléments du parcours, qui ne sont pas visibles habituellement par l'ensemble des professionnels.

3.3.5. PROTECTION DE L'INFORMATION ET PROJET

Il est nécessaire d'intégrer la protection de l'information dès l'amont du projet.

Des actions courtes peuvent être mises en œuvre, afin d'évaluer le degré de complexité, les enjeux liés à la sécurité du projet et indiquer son éligibilité, après le passage au crible de la méthodologie de gestions des risques de l'organisation.

Les étapes seront découpées en :

- Lors de l'avant-projet, au moment de l'écriture du cahier des charges par la MOA,
- Lors de l'appel d'offres et de la récolte des informations. Le taux sur la sécurité de l'information aura un coefficient discriminant important pour le choix des prestataires retenus,
- Pendant le développement du produit, s'il s'agit d'un logiciel,
- Lors de la mise en production avec le MOE,
- Tout au long du projet par un accompagnement du chef de projet dans la démarche.

Il est utile d'orienter un dialogue « sécurité » entre le MOA et le Chef de projet et de définir une politique de sécurité à appliquer à nos projets reprenant les critères de Disponibilité, Intégrité, Confidentialité, Traçabilité (voir §2.5.2 page 78) dans le respect de la réglementation et de la législation.

Cette politique définira :

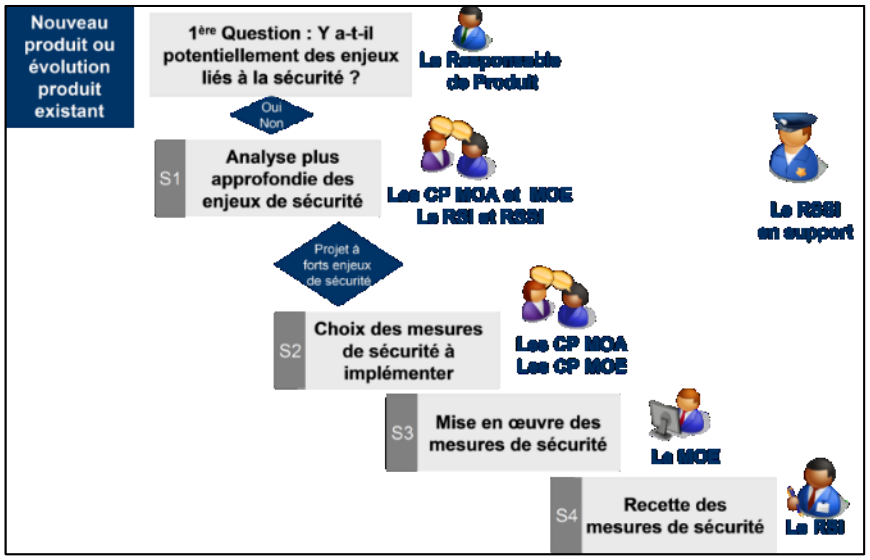
- Comment reconnaître les risques, créer et mettre en œuvre les mécaniques de sécurité afin de les réduire dont la sensibilisation des acteurs,
- Les critères d'exigence de sécurité fonctionnelle et technique,
- Les indicateurs de mesure,
- Les contrôles mis en œuvre tout au long du projet (Audit, tests d'intrusion[206]),
- La réglementation qui sera prise en compte (RGPD, brevets, propriété intellectuelle, droit d'auteur, logiciels libres, etc.).
- Comment constituer un dossier d'homologation / validation du projet

---

205 La « Joint Commission » est basée aux États-Unis ; organisme sans but lucratif. La majorité des états américains demandent aux organismes de santé son accréditation comme condition pour exercer et le remboursement des frais de santé. https://www.jointcommission.org/

206 Un test d'intrusion (« pénétration test » ou « pentest », en anglais) est une méthode d'évaluation (« audit », en anglais) de la sécurité d'un système ou d'un réseau informatique ou un Système d'information ; il est réalisé par un testeur, (« pentester », en anglais).

Nous pouvons, par exemple, développer une démarche analogue à celle-ci :



ID n° 39 exemple d'accompagnement de la sécurité sur la mise en place d'un nouveau produit. Source https://www.ysosecure.com/

3.4. MENER UNE CAMPAGNE DE SENSIBILISATION

Suivant l'organisation et le budget, la personne en charge de cette étape fera appel ou non à un prestataire externe pour l'accompagner dans la démarche. Cette aide, se matérialisera par l'apport d'outils (graphique, informatique, etc.) et de démarche intellectuelle (rédaction, interview, étude, etc.).

➔ *ETAPE 0 : QUEL PROFIL POUR SENSIBILISER LES ACTEURS DE L'ENTREPRISE ?*

Le rapport *Threat Landscape 2017* de SANS Institute Reading Room[207] indique que certains individus sont ciblés par des menaces particulières et, aussi que les acteurs de l'organisation peuvent être des « pare-feu avertis », c'est-à-dire un rempart pour la protection de la formation s'ils sont sensibilisés.

De plus en plus d'organisations, ont pris conscience de cet aspect de la sécurité et recrutent des « *Security Awareness Officer* » ou « Responsables de sensibilisation à la sécurité ». Malheureusement le service des ressources humaines se trompe en recrutant des profils, essentiellement techniques.

Il est prouvé que, plus une personne à un niveau de connaissance élevé en sécurité et, plus elle considérera que ses interlocuteurs ont un niveau similaire. Cette attitude porte le nom de « *malédiction de la connaissance* », ce qui se traduirait par « *plus une personne à une expertise élevée dans son domaine, et plus elle aura des difficultés à communiquer autour d'elle* ».

Lors du recrutement ou la nomination du « Monsieur ou Madame Sensibilisation », l'attention devra être focalisée sur les points suivants :

- Les qualités relationnelles : la personne recrutée devra aimer travailler en groupe, aimer les gens et s'intéresser aux métiers qu'elle rencontrera.

[207] SANS Institute Reading Room https://www.sans.org/reading-room/whitepapers/threats/2017-threat-landscape-survey-users-front-line-37910

- La communication et le marketing : la sensibilisation est une question de message et de mobilisation des acteurs de l'organisation. Cette personne devra être capable d'employer les termes des acteurs de l'organisation et, mettre en œuvre des outils qui soient compréhensibles par tous.
- La collaboration et la transversalité : la personne va travailler en transverse avec l'ensemble des services de l'organisation notamment, les ressources humaines, les services d'audit et de conformité, juridique, informatique, marketing et communication, la direction, les chefs de projet, le service fournisseurs, le support technique, etc.

Le comportement de la personne recrutée se résumera à sa motivation et à ses capacités et non à ses seules connaissances techniques.

Le modèle comportemental de Fogg[208] montre que trois éléments doivent converger au même moment pour qu'un comportement se produise : capacité (ou aptitude), motivation et déclencheur.

Donc le profil du « Responsable de la sensibilisation » s'orientera vers une personne ayant une formation en communication, marketing, enseignement, ventes ou relations publiques.

Nous pourrons communiquer auprès des acteurs de l'organisation, nos préoccupations et les dangers en matière de protection de l'information. Cette personne comprendra ce que nous lui demandons, car, elle n'aura pas de connaissance technique, comme les acteurs de l'organisation ! Donc elle saura adapter notre message aux différents interlocuteurs.

➔ *ETAPE 1 : QUE VEUT-ON TRANSMETTRE ET A QUI ?*

Cette question est issue de l'andragogie. La première étape se focalise sur « *que veut-on transmettre et à qui ?* » : les apprenants seront identifiés ainsi que le savoir à transmettre, adapté au public visé.

Un état des lieux de nos apprenants est dressé :

- Quel est le périmètre du poste de l'apprenant ?
- Quels sont son contexte professionnel et son écosystème ?
- Quels outils utilise-t-il ?
- Et enfin qu'elle est la connaissance que l'apprenant a de son environnement direct et indirect.

La démarche de Genba Walk guidera nos pas sur le terrain, pour faire cet inventaire et rencontrer les acteurs de l'organisation. La méthode ADKAR nous sera utile pour identifier les résistances et mener le changement.

Nous pouvons mener une sensibilisation par une approche :

- Horizontale : c'est-à-dire former un niveau hiérarchique tout secteur confondu ;
- Métier ou verticale : les apprenants sont regroupés par domaine de compétence identique,
- Suivant la résistance au changement,
- Ou en mixant les approches précédentes.

La même démarche sera menée sur l'organisation car une industrie de pointe n'a pas les mêmes problématiques de sensibilisation de son personnel qu'une banque. Ces deux secteurs sont exposés à des risques différents.

---

208 http://behaviormodel.org/index.html

À partir de ces premières constatations, nous pourrons en déduire un portrait, les savoirs et les comportements acquis et à acquérir. Après quoi nous pourrons formuler les objectifs de la formation et ce que l'apprenant devrait avoir acquis après celle-ci.

Les problématiques des différents services doivent être mentionnées, comme :

- Les services des finances, bancaire ou les courtiers (délit d'initié, fusions acquisitions, données de cartes bancaires),
- Le traitement de données stratégiques sensibles gérées par les Directions de l'organisation,
- La gestion des marchés, les ventes et les achats (offres et contrats signés),
- Les processus de l'organisation gérés par le service qualité et/ou technique,
- La protection du savoir-faire de l'organisation à travers ses brevets, sa recherche et l'innovation,
- Les données du personnel et des clients (contrats, données personnelles des clients, des fournisseurs),
- Etc.…

➔ *ETAPE 2 : LES RESSOURCES ET SUPPORTS*

Afin de prodiguer un enseignement adapté, nous allons effectuer des recherches sur les ressources disponibles, correspondants à nos objectifs de formation :

- Les personnes expérimentées sur le sujet à traiter, les cabinets spécialistes dans la sensibilisation, les institutions comme l'ANSSI, le CIGREF…
- Les manuels, rapports, infographies, articles, cours d'autoformation (formation en ligne), procédures, vidéos, jeux, sites internet, MOOC, outils interactifs et ludiques, etc.
- Les situations concrètes de mise en danger de l'information, auxquelles l'organisation aurait été confrontée, ou d'autres entreprises dans un secteur similaire.

➔ *ETAPE 3 : QUEL TYPE D'ORGANISATION*

IL EST CONSEILLE DANS L'ANDRAGOGIE D'ADAPTER NOTRE INTERVENTION A NOTRE PUBLIC ET A NOS OBJECTIFS DE FORMATION.

Les interactions seront différentes, ainsi que les échanges avec les apprenants.

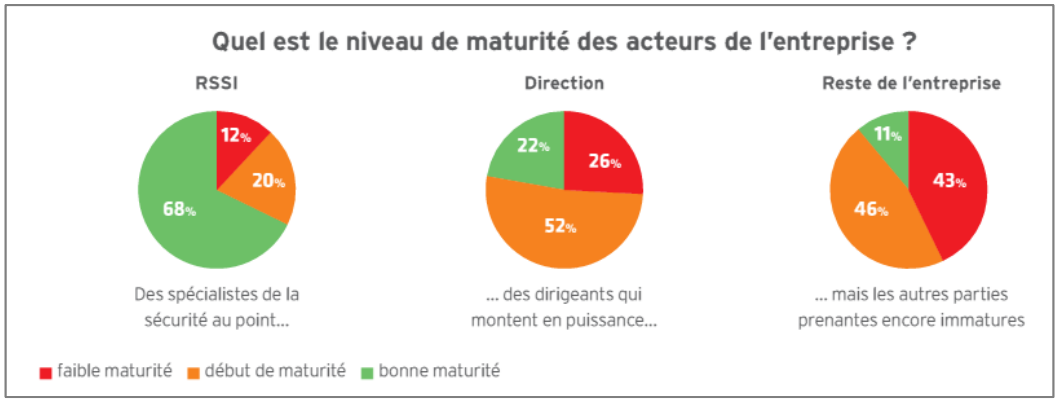
Un ensemble de questions se poseront avant d'organiser les campagnes et les supports pédagogiques qui iront de pair, comme :

- L'intervention d'un spécialiste auprès d'un plus grand nombre d'acteurs de l'organisation est-elle utile ?
- La venue d'un spécialiste technique, qui fera des démonstrations de clonage de badge ou de piratage d'ordiphone, intéressera-t-il l'ensemble de notre population ?
- Etc…

SECTORISER DES ACTEURS A SENSIBILISER

Qui sont les utilisateurs ?

Il est conseillé à la personne responsable des campagnes de sensibilisation ou des formations à la sécurité, de connaître les acteurs de l'organisation, leur métier, les risques auxquelles ils sont exposés, leur préoccupation et leur niveau de maturité vis-à-vis de la sécurité de l'information, afin de communiquer de manière ciblée.

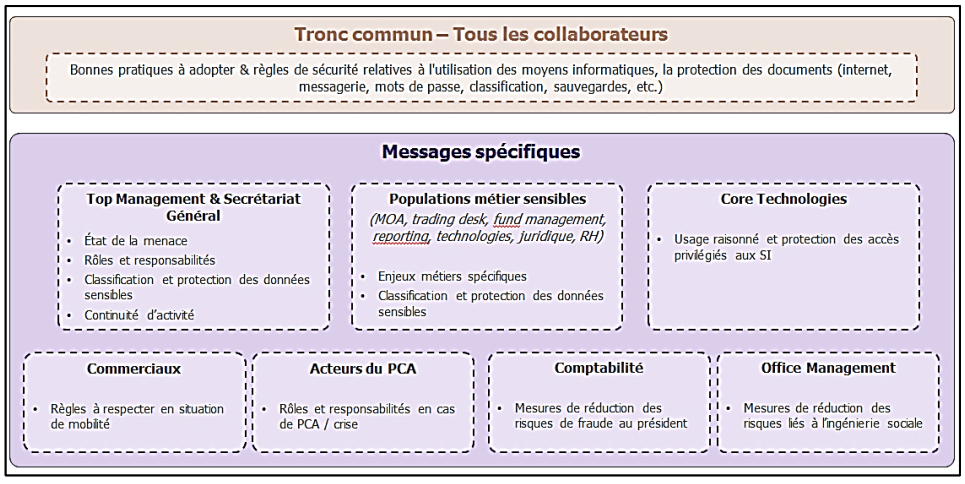


ID n° 40 Guide de la cyber sécurité 2016 Alliancy Etude Deloitte 2016

La sectorisation peut s'opérer par :

- Groupe de personnes ou groupe d'intérêt (communauté de pratique) : service DRH, DSI, Financier, accueil du public, organisation d'évènements, etc.
- Typologie des personnes : administrative, technique, médecin, soignant, informatique, nouveaux arrivants, manager, chefs de projets, développeurs…
- Les personnes clés, comme :
- Les médecins pour un hôpital car ils manipulent des données de patients,
- Les automaticiens dans le secteur industriel,
- Les membres du Comité de direction,
- Les Direction de recherche et développement
- Etc.

Le cabinet Carmignac a choisi de sectoriser ses apprenants par métier :

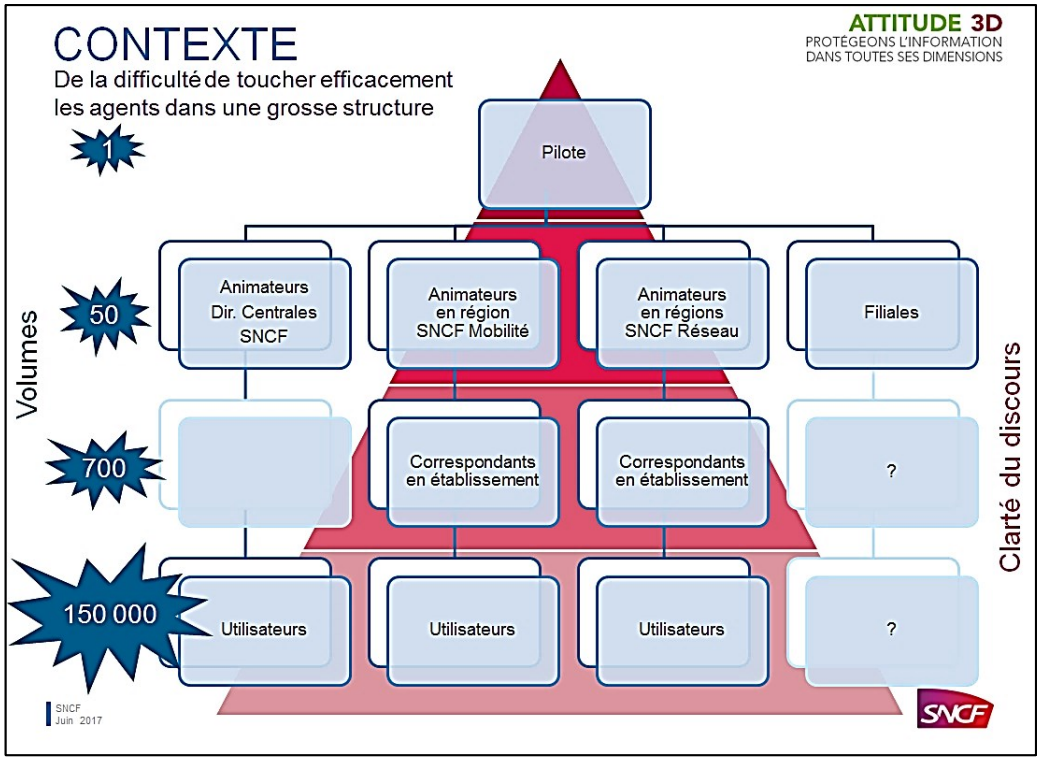


ID n° 41 exemple de la sectorisation des acteurs du cabinet Carmignac à sensibiliser

MISE EN PLACE D'UN RESEAU DE RELAIS DANS LES SERVICES

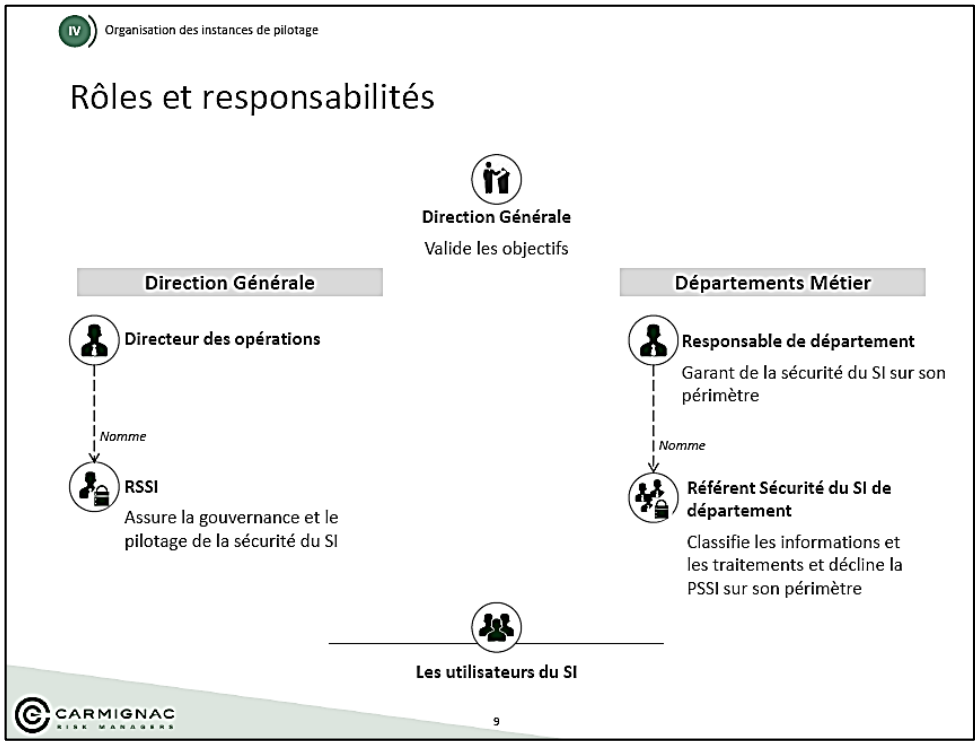
Le responsable de la sécurité des informations ou le RSSI seul, ne peut rien, il s'appuie sur des relais dans l'organisation.

La SNCF, par exemple, se repose sur des animateurs, pour faire passer ses messages, distribuer les supports de communications, les jeux etc.



ID n° 42 Organisation des relais de la SNCF

Le cabinet Carmignac s'appuie sur les responsables de département, qui sont garants de la sécurité du système d'information sur leur périmètre. Ils nomment un référent de la sécurité dans leur département.



ID n° 43 Relais et appui dans les services du cabinet Carmignac

➔ *ETAPE 4 : CAHIER DES CHARGES*

Nous avons l'ensemble des éléments nécessaire, à la rédaction de notre cahier des charges, de notre prochaine campagne de sensibilisation.

Ce document est un élément contractuel entre le CODIR et/ou un prestataire externe.

Celui-ci décrira :

- L'organisation de l'entreprise (nombre et catégories des personnes concernées).
- L'objectif de notre campagne, sera notre point central, lors de la rédaction. Celui-ci mentionnera les savoirs à acquérir et par qui.
- La stratégie d'organisation des formations que nous souhaitons mettre en place,
- Les stratégies d'enseignement qui seront utilisées.
- Les objectifs de la formation, seront exprimés, de façon synthétique, les comportements qui à acquérir et à mettre en œuvre lors de la vie professionnelle des acteurs de l'organisation.

➔ *ETAPE 5 : LE PROGRAMME DE LA CAMPAGNE*

Cette étape sera la rédaction du programme de la campagne et de quelle façon nous allons organiser la sensibilisation.

Suivant notre cahier des charges et les décisions arrêtées en comité de direction, nous pourrons faire appel à un prestataire externe qui rédigera le déroulé du programme, avec notre concours.

EXPLIQUER POURQUOI LES INFORMATIONS D'UNE ORGANISATION SONT A PROTEGER

La première étape consiste à expliquer, pourquoi les informations de l'organisation sont à protéger, qu'elles sont les menaces qui pèsent sur celles-ci et diffuser le discours auprès des acteurs.

Le but est que les personnels comprennent les enjeux et qu'ils se les approprient, sinon, ils ne les suivront pas. La sensibilisation sera menée comme un projet avec sa partie de conduite du changement.

La méthode ADKAR pourra servir de fil conducteur dans la mise en place de la feuille de route à établir pour mener la campagne. Nous pourrons nous inspirer de la feuille de route réalisée par Pascal Le Deley (ID n° 36 page 99).

L'élément le plus important est la compréhension du discours.

Ce point assimilé par l'ensemble des acteurs de l'organisation, on pourra se focaliser sur les bonnes pratiques à adopter en partant des menaces identifiées. Celles-ci varient suivant les organisations et les moyens de sécurisation en place.

Les campagnes de sensibilisation s'adapteront aux règles en vigueur dans les organisations (PGSSI, PSSI, Chartes) et aux outils utilisés, afin que les formations soient opérantes.

Les supports seront adaptés aux populations de l'organisation (administrateurs, développeurs, utilisateurs « fixes », utilisateurs itinérants, services RH, Direction générale, Direction financière), tout en ayant un tronc commun.

Une attention toute particulière sera apportée aux personnels de la DSI, qui, contrairement à ce que l'on pourrait imaginer, ne sont pas plus aguerris en matière de sécurité des informations. Cette catégorie de personnel dispose de plus de droits que les utilisateurs « classiques » et

représente un risque.

Les sujets d'actualités et la transposition à la sphère privée viendront renforcer les messages. Nous nous appuierons, également, sur les incidents de sécurité auxquels l'organisation a été confrontée. Cette démarche peut déclencher un cercle vertueux, car les acteurs sensibilisés, pourront jouer le rôle de « lanceurs d'alerte », en détectant des comportements anormaux.

Inventer des slogans facilement assimilables (exemple « Mobilité Sécurité = Sûreté ! »), prendre exemple sur les Haïkus[209] ou les slogans des panneaux d'autoroute, courts et percutants (exemple : « ceinture attachée = vie sauvée ») et varier les approches. Nous nous appuierons sur la méthode de Design Thinking, les acteurs seront les inventeurs de ces slogans, pour mieux se les approprier.

Les sujets de base et parlant aux acteurs de l'organisation pourront être traités comme :

- La gestion des mots de passe : gérer les mots de passe de manière à protéger l'accès aux informations, utiliser des outils comme les coffres-forts de mots de passe, créer un mot de passe fort.
- Les périphériques et le poste de travail : les disques durs externes, les clés USB, etc.
- Messagerie électronique : identifier des risques et comment les éviter (exemple : phishing).
- Internet : identifier des risques et comment les éviter
- Protections des données : rappels des aspects juridiques liés à l'utilisation du système d'information et rappels des règles à suivre (charte, PSSI, RGPD).
- Mobilité : comment protéger son ordinateur ou son ordiphone lorsque l'on est en voyage pour des raisons professionnelles ou personnelles (exemple : réseau Wifi public).
- Réseaux sociaux : comment protéger ses données personnelles et son identité sur les principaux réseaux sociaux. Les paramètres de sécurité et de confidentialité des réseaux sociaux principaux (LinkedIn, Facebook, Twitter, etc.).

> *« Il faut mettre le salarié au cœur de la démarche de sécurité. C'est un peu plus facile aujourd'hui qu'il y a 10 ans car les utilisateurs se sentent davantage concernés à titre personnel. Il faut donc parler d'eux, de leur rôle en tant que citoyen pour protéger leurs données personnelles ».*
>
> *« Il peut y avoir des programmes de fonds. Dans ce cas, il est nécessaire de s'appuyer sur les RH car cela s'inscrit dans une démarche globale de formation, comme l'incendie par exemple. À cette occasion, le DRH peut mettre en place une plate-forme d'e-learning ou un dispositif de suivi de session ».*
>
> *Jean-François LOUAPRE, RSSI et vice-président du CESIN (Club des experts de la sécurité de l'information et du numérique).*

RESPONSABILISER LES ACTEURS EXTERNES

L'organisation travaille avec des partenaires externes (éditeurs de logiciel, Datacenter, maintenance de matériel, etc.). Ces personnes seront prises en compte lors de la mise en place de la sécurisation des informations de l'organisation, notamment lors de la signature de contrat ou d'accords commerciaux.

La sécurisation mise en place au sein de l'organisation sera mentionnée dès l'écriture du cahier des charges, l'appel d'offres et dans le contrat liant les parties.

---

[209] Petit poème japonais, extrêmement bref visant à dire et célébrer l'évanescence des choses (source https://fr.wikipedia.org/wiki/Ha%C3%AFku)

Les critères de sécurité sont discriminants vis-à-vis du choix d'un prestataire.

Un PAS (Plan d'Assurance Sécurité) sera mis en place entre les deux parties, reprenant l'ensemble des points de sécurité (de la connexion au système d'information de l'organisation, au respect des données personnelles auxquelles le prestataire pourrait avoir accès). Le RGPD, pourra servir de tremplin réglementaire pour mettre en œuvre ce PAS, sachant que les prestataires sont soumis, eux aussi à ce règlement.

Une labellisation les fournisseurs de produits ou services de SSI peut être mise en place au sein de l'organisation et se référer aux entreprises qualifiées par l'ANSSI. Celles-ci sont soumises à un protocole de labellisation stricte répondant à un haut niveau de sécurité[210].

3.5. SUPPORT DE COMMUNICATION ET OUTILS

Il existe différents moyens et médias permettant de sensibiliser les utilisateurs à la sécurité. Ils ont tous des avantages et des inconvénients.

Une variété de ces supports de communication sera utilisée dans notre plan de sensibilisation (voir le retour des professionnels page 71) et sera renouvelée d'une année sur l'autre, afin de diversifier l'enseignement de la protection de l'information et garder un côté attrayant ou ludique.

➔ *QUE RETIENT-ON ?*

Les activités combinées sont plus efficaces que les activités pratiquées isolément.

La pratique de la « *formation action* », inventée par Reginald Revans[211] et dont le concept a été développé en 1940 au Royaume Uni a pour objectif d'améliorer la productivité des apprenants, et permettre aux adultes d'analyser une action réalisée, de visualiser les points de correction ou d'amélioration futurs.

Par exemple : les activités « Lire », « Entendre » et « Voir » permettent de retenir, au plus, 30 % de ce qui est enseigné. Ce pourcentage augmente si vous combinez des actions « Voir et Entendre ».

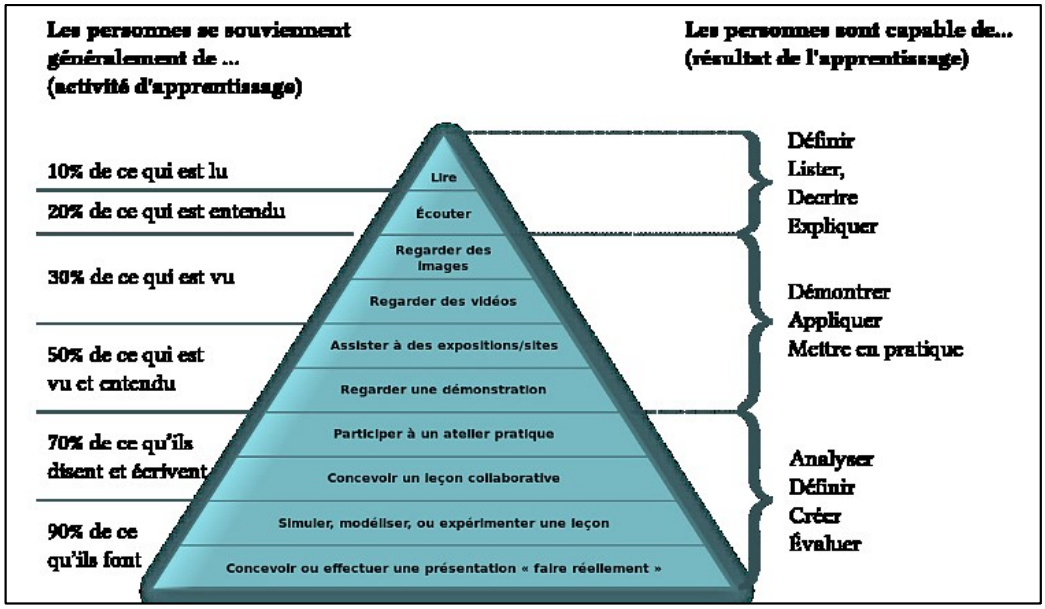
Combiner un ensemble de supports, visuels, sonores et créer de l'interaction permettra aux acteurs formés et sensibilisés, de retenir un maximum d'information[212].

---

210 La qualification est la recommandation par l'État français de produits ou services de cybersécurité éprouvés et approuvés par l'ANSSI. Elle atteste de leur conformité aux exigences règlementaires, techniques et de sécurité promue par l'ANSSI en apportant une garantie de robustesse du produit et de compétence du prestataire de service, et d'engagement du fournisseur de solutions à respecter des critères de confiance. http://www.ssi.gouv.fr/entreprise/qualifications/

211 Reginald William Revans était un professeur, administrateur et consultant britannique, pionnier dans l'usage de la formation-action.

212 Source http://www.icea.qc.ca/site/fr/services/formation-en-milieu-de-travail



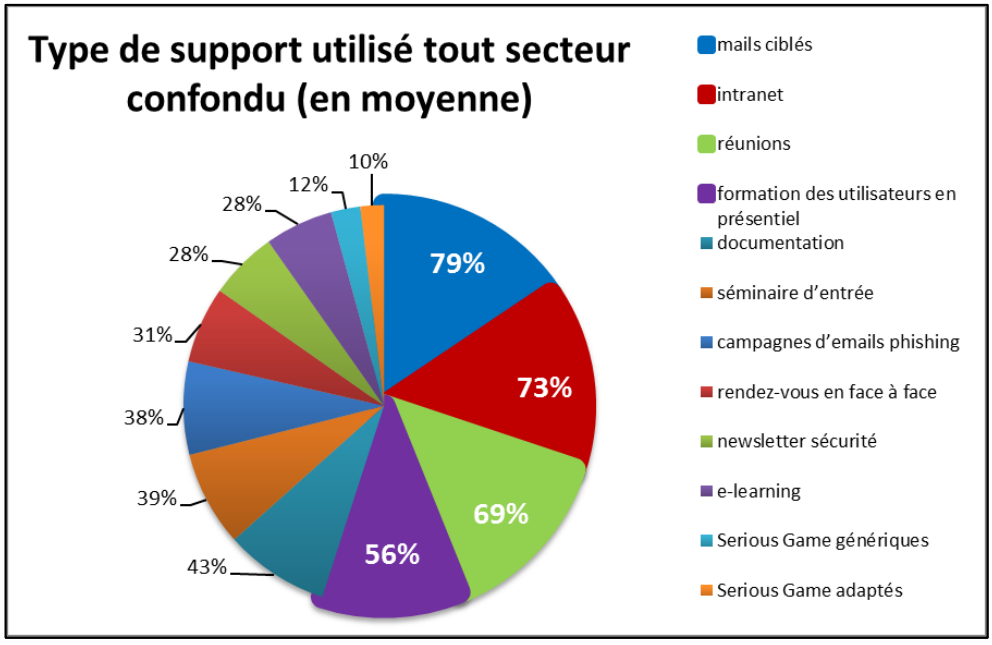
ID n° 44 Interprétation du triangle d'apprentissage d'Edgar Dale par Psychoslave

➔ MEDIAS DE COMMUNICATION

À la suite de l'enquête menée auprès des RSSI (voir page 71) il ressort que le support le plus utilisé est le courriel ciblé. Les RSSI profitent de l'actualité pour rebondir sur les évènements et apporter des faits, par courriel, auprès des acteurs de l'entreprise.

Vient ensuite l'intranet. Celui-ci est souvent paramétré comme la page par défaut du navigateur internet, des postes utilisateurs. Les messages à faire passer sont visibles dès qu'un utilisateur souhaite se rendre sur internet.

Les interventions en réunions talonnent les deux précédents supports, avec les formations en présentiel. Les personnes bénéficient de retour immédiat en face-à-face de la part du RSSI ou du formateur. Une interaction entre les participants se met en place.



ID n° 45 supports utilisés tout secteur économique confondu pour sensibiliser les acteurs. Retour de l'enquête Annexe n°18

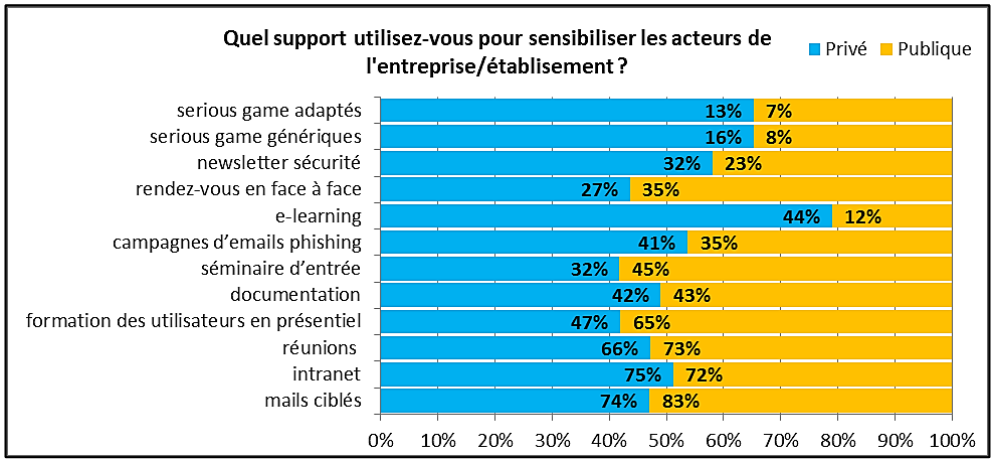
LE DECOUPAGE PAR SECTEUR PRIVE ET PUBLIC FAIT RESSORTIR DES ECARTS SUR L'USAGE DES OUTILS DE SENSIBILISATION.

La pédagogie aux nouvelles technologies, les dangers des IOT, etc. Est aussi un moyen d'informer les utilisateurs au travers des bulletins d'information spécialisés en sécurité (32 % dans le privé et 23 % dans le public).

La formation en ligne est fortement employée dans le privé (44 % contre 12 % dans le public), ou l'emploi de « *Serious game* », dont l'aspect ludique est mis en avant auprès des apprenants (13 % et 16 % pour le privé contre 7 % et 8 %, seulement pour le public).

La formation en ligne offre de la souplesse pour les apprenants et un moyen de contrôle de la compréhension et de l'assimilation de la protection de l'information. Ce type d'approche représente un budget que le secteur public n'est pas prêt à dépenser.

Le secteur public reste traditionnel dans son approche de la sensibilisation, en privilégiant, la formation des utilisateurs en présentiel (65 %) et les rendez-vous en face-à-face (35 %).



ID n° 46 découpage des supports les plus utilisés dans le public et privé. Retour de l'enquête

Les réponses, ne mentionnant pas le secteur public ou privé, ont été éliminées du calcul ci-dessus (Non indiqué 13, Privé 96, Publique 60).

➔ *GADGETS*[213]

Les utilisateurs sont sensibles aux objets « publicitaires », ils ont l'impression de faire partie de l'élite ! Ou du moins ils peuvent prouver, via l'objet, qu'ils sont inscrits dans le cercle des « *sachants* ».

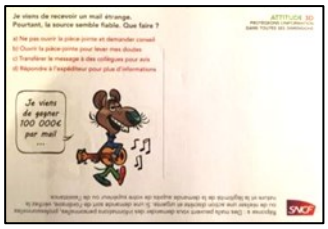
La distribution de gadgets, peut joindre l'utile à l'agréable, comme des clefs sécurisées, des tapis de souris ou post-it avec un message intégré.

L'objet reste et est vu et manipulé par les personnes qui visitent leur collègue dans leur bureau (voir Annexe n°14 page 189).

[213] Un goodies est le terme anglais pour désigner un cadeau publicitaire. Les goodies sont distribués dans le cadre d'actions de marketing. Ils peuvent notamment prendre la forme de stylos, jetons caddie, bloc-notes, …

ID n° 47 Clef USB sécurisée

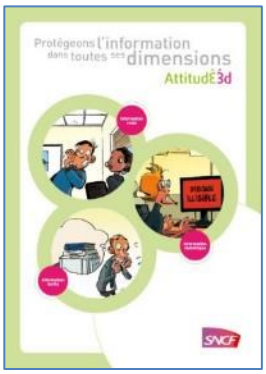
ID n° 48 Tapis de souris



ID n° 49 Post-it

ID n° 50 Gobelet

Les bandes dessinées sont très appréciées, car elles permettent de faire passer un message de manière ludique. Celles-ci peuvent comporter plusieurs tomes, au vu de l'actualité ou des campagnes de sensibilisation.



ID n° 51 Bande dessinée SNCF

ID n° 52 JM UCCIANI
Dessinateur http://www.ucciani-dessins.com/securite-du-systeme-d-information-ssi/

ID n° 53 Commistrip
http://www.commitstrip.com/fr/

➔ *LOGO LUDIQUE : CREATION D'UNE IDENTITE DU POLE DE SENSIBILISATION*

Créer une identité de service de sensibilisation peut faciliter la diffusion des messages. Immédiatement, nos interlocuteurs reconnaîtront la provenance de l'information. Ce logo permet de transmettre, un message par le biais d'une communication visuelle.

Un logo peut être créé avec une forme et des couleurs adaptées à l'identité et la fonction du service (exemple un bouclier évoquera la protection et les couleurs sont en harmonie avec le logo de l'organisation).

La forme du logo, les couleurs et les caractères seront adaptés en fonction du message que l'on souhaite afficher. Celui-ci sera unique, durable dans le temps, pour la crédibilité, et aussi car la création d'un logo représente un coût, qui peut être élevé.

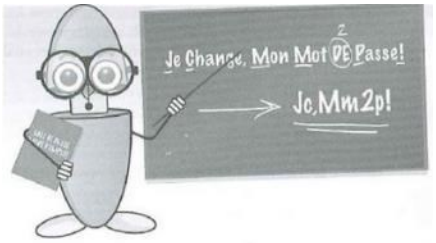
A.P.I
Acteur de la Protection de l'Information
SSI GCS du Chalonnais

ID n° 54 logo du service RSSI GHT du Nord Morvan[214]

Logo des entités du GHT

GROUPEMENT HOSPITALIER DE TERRITOIRE SAÔNE ET LOIRE BRESSE - MORVAN

GCS du Chalonnais
Groupement de coopération sanitaire



ID n° 56 Bernard Foray, élu RSSI de l'année 2010 par le magazine 01 Informatique,

Attitude 3d

ID n° 55 logo du service de sensibilisation de la SNCF

SNCF

voyages-sncf.com

ID n° 57 protegetonordi.com

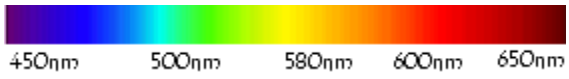
➔ *LES COULEURS POUR QUEL MESSAGE*

Nous retenons et assimilons mieux la couleur que les formes et les mots.

QUE VOIT L'ŒIL HUMAIN ?

Chaque couleur émet un rayonnement lumineux sur une certaine longueur d'onde.

L'œil humain est capable de saisir des couleurs dont la longueur d'onde si situe entre 380 et 780 nanomètres. L'ensemble des longueurs d'onde visibles par l'œil humain est appelé « spectre visible » :



LA SYMBOLIQUE DES COULEURS

Des images et des symboles sont attachés aux couleurs. Ceux-ci sont différents suivant les cultures, le moment et les circonstances. Elles peuvent être classées par thème avec leur symbolique.

Chaque couleur a sa propre signification et qui conditionne notre ressenti[215].

Les couleurs dites fondamentales (couleurs de l'arc-en-ciel) sont au nombre de sept : Violet, Indigo, Bleu, Vert, Jaune, Orange, Rouge.

---

214 Créé par S. Ducharne

215 http://tiprof.fr/HTML-CSS-court/ressources/Miroirs/www.cci-grenoble.artxtra.info/formation/pdf/symbolique_couleurs.pdf

COULEUR	SYMBOLIQUE
Blanc	Le blanc symbolise avant tout l'union, la pureté. Il rappelle la froideur, le silence.
Bleu	Le bleu représente la pensée, la paix c'est l'une des couleurs les plus pures. Il peut évoquer l'infini (ciel). Au Moyen Âge, le pigment bleu lapis-lazuli, était plus cher que l'or. Il était le symbole de pouvoir des rois. Thématiques : Informatique, high-tech, médecine.
Gris	Le gris est un mélange de noir et le blanc. Couleur sobre, le gris inspire la tristesse et paradoxalement il possède une connotation de modernisme
Jaune	Couleur de lumière, le jaune procure un effet intense et riche, et inspire la jeunesse. Le jaune attire l'attention, il est utilisé pour signaler et informer.
Noir	Le noir inspire la fin, la détresse. Ces symboliques liées à la mort lui confèrent des connotations négatives. Souvent associé au produit de luxe (élégance).
Orange	Avec une très forte visibilité, la couleur orange stimule. Souvent utilisée avec une couleur foncée pour exprimer un contraste. L'orange oscille entre les connotations du jaune et du rouge (couleurs qui une fois mélangées donnent l'orange). En ce sens, elle peut être employée pour signifier la joie et la chaleur (comme le jaune), la passion et la fougue (comme le rouge), mais toujours à des degrés moindres.
Rouge	Couleur chaude par excellence, le rouge évoque, l'action, la passion, la sensualité et le désir. C'est la couleur du sang et du feu. Le rouge a un impact certain sur nos fonctions physiologiques. C'est une couleur joyeuse
Vert	La couleur verte rassure et rafraîchie, elle évoque tour à tour la nature, la santé et le savoir (l'habit vert des académiciens).
Violet	Mélange de bleu et de rouge, le violet renvoi une connotation magique tout en insistant sur la mélancolie.

ID n° 58 Signification des couleurs fondamentales source https://www.toutes-les-couleurs.com/

Faber Birren[216], un des pionniers de la recherche sur la couleur, a réalisé un sondage, dont le résultat indique quel est le sentiment que les personnes interrogées associent à quelle couleur[217] :

SENTIMENT RESSENTI	COULEUR
Confiance	Bleu
Sécurité	Bleu
Vitesse	Rouge
Qualité médiocre	Orange (le jaune se classe juste derrière)
Qualité supérieure	Noir
Haute technologie	Le noir déclasse à peine le bleu et le gris, à égalité
Fiabilité	Bleu
Courage	Pourpre et rouge
Peur/Terreur	Rouge
Plaisir	Orange (le jaune se classe juste derrière

SYMBOLIQUE DES COULEURS SUIVANT LE PAYS

CULTURE	ROUGE	BLEU	VERT	JAUNE	BLANC
Etats Unis	Danger	Masculinité	Sécurité	Lâcheté	Pureté
France	Aristocratie	Liberté Paix	Criminalité	Temporaire Provisoire	Neutralité
Egypte	Mort	Vertu Foi Vérité	Fertilité Force	Joie Bonheur Prospérité	Joie Gaieté
Inde	Vie Créativité		Prospérité Fertilité	Succès	Mort Pureté
Japon	Agressivité Danger	Traîtrise	Futur Jeunesse énergie	Grâce Noblesse	Mort
Chine	Joie Gaieté	Paradis Nuages	Dynastie Ming	Naissance	Mort Pureté

[216] Auteur du *livre Color Psychology and Color Therapy* http://www.colorsystem.com/?page_id=922&lang=fr. Faber Birren (1900-1988) a étudié la façon dont la couleur affecte notre humeur et les effets de la couleur sur le corps lui-même.

[217] Source https://www.canadapost.ca/

CULTURE	ROUGE	BLEU	VERT	JAUNE	BLANC
			Paradis Nuages	Richesse Pouvoir	

ID n° 59 symbolique des couleurs suivant le filtre culturel

On peut aussi parler du violet qui, a une valeur essentielle dans beaucoup de cultures. Par exemple chez les Soviétiques elle était associée au glorieux rouge sang et chez les musulmans c'est une couleur maudite.

PHYSIOLOGIE DE LA COULEUR

La couleur est sensation.

Les couleurs émettent des ondes et, ont un impact différent sur celui ou celle qui les regarde, à cause de leur contraste, leur intensité et leur effet spatial. Celles ayant les plus grandes longueurs d'onde, sont perçues plus rapidement. C'est pourquoi nous avons la sensation que le rouge « saute aux yeux » et que le bleu est plus « apaisant ». Les couleurs claires ont la capacité « d'agrandir l'espace » incitent au calme, à la réflexion, à la détente tandis que les couleurs foncées ont tendances à « rétrécir l'espace ».

L'institut Color Research[218] a effectué des recherches en partenariat avec l'université de Winnipeg (Canada) sur l'influence de la couleur sur les consommateurs. Le résultat des recherches a démontré que les personnes étudiées ont besoin de 90 seconds maximums pour se forger un avis sur la valeur, la fiabilité, la qualité… D'un produit et que la couleur compte pour 62 % à 90 % dans le résultat. La couleur a une grande influence sur notre perception et nos comportements, face à une marque.

L'histoire de l'humanité est influencée par les couleurs primaires (rouge, vert et bleu), qui, depuis le départ de notre existence, ont rythmé notre vie :

- Le rouge signifie la vie, l'action,
- Le bleu, la couleur du ciel, qui devient bleu nuit lorsque le soleil est couché et synonyme d'apaisement et de tranquillité,
- Le vert est associé à la fraîcheur et l'abondance de nourriture, il est associé à l'évolution[219].

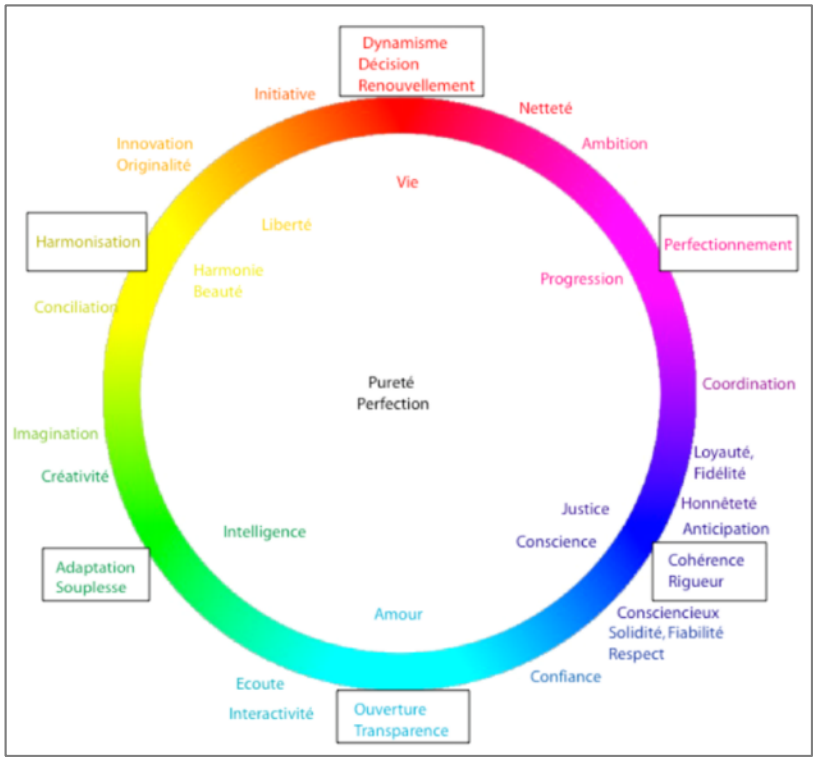
Notre interprétation, actuelle des couleurs, est guidée par les situations que notre espèce a vécues depuis des millions d'années.

[218] Division de Color Communications Inc. http://www.ccicolor.com/

[219] Source : « La tension interne à la cohésion informationnelle » thèse de M. Yves Chaumette. HAL Id: tel-00945803 https://tel.archives-ouvertes.fr/tel-00945803

QUALITE ET COULEUR

Une qualité peut être associée à une couleur et disposée sur un cercle chromatique.



ID n° 60 Les valeurs fondamentales situées dans le cercle chromatique. « La qualité au-delà des mots » d'Yves Chaumette

> *Cette représentation est conforme à la vision d'un cycle avec la raison d'être au centre, l'activité à l'extérieur et la qualité comme le rayon du cercle. Le schéma ci-dessus représente dans le cercle les raisons de vivre, les valeurs fondamentales, d'une manière semblable à la carte du monde, proposée par certains artisans de la PNL (S. Tenenbaum).*

LES AXES	DEFINITION DES AXES	MOTS ASSOCIES
Dynamisme	Capacité à se renouveler, donc la remise en cause des orientations et la mise en œuvre des moyens.	Mots associés : valeur, finalité, synthèse, recul, élan, proactif, force de proposition, concision, fermeté, décision, priorité, tonique, priorités, concision, direction, netteté
Perfectionnement	Capacité à améliorer un processus, des activités	Mots associés : améliorer, bilan, suivi, capitaliser, mieux, plus élevé, perfectionner, régler, niveau, idéal, Enthousiasme
Cohérence rigueur	Capacité de suivre une ligne déterminée, de maintenir une logique avec précision	Mots associés : Logique, démarche, méthode, anticipation, précision, exigence, méticuleux, pointer, étudier, suivre, vérifier, anticiper, conformité, fixité, planifier
Ouverture transparence	Capacité de relier (accepter, inclure) des faits, des idées, des partenaires	Mots associés : échange, liens, écoute, partage, cordialité, curiosité, interagir, convivialité, cordialité, réseau, lien, accommodant, réceptif, sociable

LES AXES	DEFINITION DES AXES	MOTS ASSOCIES
Adaptation	Capacité de réagir en fonction de la demande, du contexte, ou du partenaire	Mots associés : créativité, réactivité, souplesse, mobilité, curiosité, fantaisie, flexibilité, évoluer, réactif, sollicitation, imaginatif, jetable, mobile, portable, léger, sur mesure, opportun
Harmonisation complémentarité	Capacité de parvenir à un accord, de s'enrichir grâce aux différences.	Mots associés : alternatives, diversité, contraste, opposition, accord, convergence, différence, enrichissement, hétérogène, autre, confronter, approfondir, humour, analogie, comparaison, conflit, divergence, adverse, original

ID n° 61 signification des couleurs. Source Evalcolor d'Yves Chaumette

Le choix des couleurs influencera la perception des acteurs de l'organisation quant à la compréhension des messages que l'on souhaite leur transmettre. Elles ont aussi des conséquences, sur l'engagement, de ceux-ci envers notre contenu, et ce, peu importe le support utilisé.

Même le meilleur contenu, peut nous empêcher d'atteindre nos objectifs si, celui-ci affiche des couleurs qui transmettent un message différent de celui qu'il est censé passer.

➔ *QU'ELLES SONT LES METHODES DE SENSIBILISATION LES PLUS EFFICACES ? ET POURQUOI ?*

Durant l'enquête, nous avons demandé « *Selon vous, qu'elles sont les méthodes de sensibilisation les plus efficaces ? Et pourquoi ?* »

Le secteur privé a mis en avant l'efficacité de la formation en ligne et des serious game pour les jeunes générations. Certains rendent obligatoires les formations en formation en ligne semestriellement, faute de quoi les utilisateurs perdent l'accès à internet !

Comme le cabinet Carmignac, qui rend obligatoire ce type de support de formation auprès de ses collaborateurs commerciaux (M. Onder KELES, RSSI de Carmignac). Le règlement des marchés oblige au respect de règles (blanchiment d'argent), c'est un support qui permet de former et contrôler, que tous les collaborateurs concernés, ont suivi la formation.

La formation en ligne permet de proposer plusieurs modules, courts, répartis tout au long de l'année ; c'est un avantage. Les modules en ligne, répartis dans le temps, permettent d'assurer une sensibilisation continue et les utilisateurs gèrent leur formation à leur rythme.

Un témoignage indique que « *Ce qui marche bien est la répétition (formation en ligne annuelle, type bourrage de crâne à partir de situations réelles d'entreprise)* ».

Les serious game fonctionnent pour modifier les comportements mais doivent être reliés aux autres modes de communication et accompagner du responsable de la protection de l'information (voir heutagogie §3.2.4 page 86).

D'autres témoignages viennent compléter le tableau :

- **M. Fabrice NERACOULIS, Responsable de la sensibilisation de la SNCF :**

> *Les médias de communication peuvent être l'Intranet, le courriel mais aussi des documents, tels que la charte informatique, que l'on n'oubliera pas de communiquer dès l'arrivée dans l'organisation.*

> *Il convient de ne pas submerger l'utilisateur d'informations (trop d'informations ou fréquence trop élevée) sans quoi, il ne lira pas ou plus le contenu.*
>
> *La communication peut également se faire via des panneaux, mais cela demande un peu plus de logistique et l'information est limitée. Il faudra donc utiliser ce média pour des campagnes bien ciblées et pour des problématiques identifiées et impactant pour l'organisation.*
>
> *Par exemple, à l'arrivée des vacances, on peut redire qu'un mot de passe est personnel et ne pas le donner à ses collègues.*

- **Emmanuel Garnier, responsable sécurité des systèmes d'information de Systalians :**

> *Passer du temps pour améliorer le comportement des gens en termes de sécurité est beaucoup plus rentable que la mise en place d'outils. Nous avons monté un programme de sensibilisation en présentiel, qui a été suivi par toutes les personnes ayant un accès au système d'information, salariés comme prestataires.*
>
> *Nous continuons à faire une dizaine de sessions par an pour les nouveaux arrivants. Nous leur donnons le vocabulaire, leur parlons menaces, attaques et gestion des risques. Puis, pendant une heure et demie, nous abordons les bons comportements à avoir. Nous montrons concrètement comment il est facile de découvrir un mot de passe qui n'est pas assez robuste. Cela marque les esprits !*
>
> *Pour faire des rappels réguliers, j'écris au moins un bulletin de veille par mois sur des thématiques très différentes : sécuriser sa connexion Wi-Fi à la maison, les outils de gestion de risques, etc.*
>
> *Nous donnons toujours des exemples pour illustrer nos propos. Sur notre intranet, nous utilisons les jeux sous forme de questionnaire de l'éditeur Hapsys, mais aussi, depuis fin 2009, nous mettons en ligne chaque mois deux petits films qui traitent de sécurité.*[220]

3.6. CONCLUSION

La réussite du projet est liée à :

- L'appropriation des acteurs de l'organisation à la protection de l'information du système d'information. Nous devons expliquer pourquoi il est important de protéger l'organisation, afin d'augmenter les chances de réussite du projet.
- Le discours apporté (trop de techniques vont perdre les acteurs qui ne comprendront rien),
- L'adaptation des formations aux publics visés,
- Le dynamisme des approches (formation en ligne, jeux, etc.)
- Une conduite du changement menée avec délicatesse et sur le terrain.
- Notre marketing ! Les messages à faire passer dépendent des mots et, également de « l'emballage » dans lesquels ils seront présentés.
- Prendre le temps d'expliquer notre démarche, au service de communication de notre organisation, pour déterminer les valeurs et les caractéristiques, auxquels on souhaite associer l'action de sensibilisation de notre organisation.

Cette démarche nous aidera à structurer notre message et la forme des supports de communication. Le service communication pourra nous apporter leur expertise, quant à la connaissance des fondements de notre organisation et de sa composante humaine.

---

220 Emmanuel Garnier, responsable sécurité des systèmes d'information de Systalians, GIE informatique de Réunica et Bayard retraite prévoyance http://www.argusdelassurance.com/acteurs/securite-des-systemes-d-information-la-faille-est-souvent-humaine.

CHAPITRE 4
MESURER LA SENSIBILISATION

« J'entends et j'oublie.
Je vois et je me souviens.
Je fais et je comprends. »
Confucius[221]

[221] Confucius est un des personnages historiques qui a le plus marqué la civilisation chinoise et est considéré comme le premier « *éducateur* » de la Chine. Son enseignement a donné naissance au confucianisme.

4.1. INTRODUCTION

L'évaluation nous permet, de vérifier les acquis de savoirs, de savoir-faire, et de détecter les difficultés de l'auditoire, quant aux situations rencontrées et/ou le discours que nous tenons.

4.2. MESURE DE LA SENSIBILISATION

Les actions de sensibilisation effectuées auprès des acteurs de l'organisation seront mesurées afin d'apprécier la qualité de notre travail à partir de l'objectif que nous nous étions fixé, et, d'entrevoir des remédiations, si nécessaire, pour les prochaines campagnes.

La remédiation consiste à renouveler des séances d'apprentissage ou de sensibilisation qui sont basées sur les mêmes objectifs, à partir de nouveaux supports de formation. Et ce, jusqu'à ce que nous ayons atteint nos objectifs. Du côté des apprenants, l'évaluation leur permet de mesurer leurs acquis et le chemin qui les sépare de l'objectif final.

Des outils peuvent être utilisés lors de campagne (exemple : campagne de phishing). Des organisations comme *CyberReady*[222], compare leur méthode à celle de la ligue majeure de baseball des Etats-Unis appelée *sabermétrie*[223].

Des statistiques sont produites à partir de nombreux indicateurs complexes qui sont analysés et décortiqués. Les statistiques précédentes de la ligue majeure de baseball, étaient uniquement basées sur l'empirisme. Au vu du nombre de paris et d'argent en jeu, d'autres techniques, plus fiables, ont été mises en œuvre.

CybeReady, ou d'autres sociétés, proposent de fournir le taux de clic ou, le nombre de personnes ayant consulté les sites Web, à partir de liens contenus dans les courriels de campagne de phishing.

La prudence s'impose dans l'analyse qui en découle ! Il peut s'agir de toujours les mêmes personnes qui cliquent sur les courriels frauduleux ou, de personnes différentes à chaque campagne. Donc nous devons prendre en compte, de manière précise, la période, la variété des courriels et la population ayant reçu les messages afin d'analyser la situation réelle.

Lors de nos mesures, nous devrons déterminer si nous analysons le même groupe de personnes ou s'il y a de nouveaux employés inclus dans ces mêmes groupes, car cela faussera notre résultat sur la comparaison des progrès effectués ou non.

Des entreprises spécialisées dans la mesure de campagne, incluent des algorithmes qui se basent sur le big data en utilisant le taux de clic et d'autres indicateurs, pour en déduire le taux d'apprentissage réel des acteurs de l'organisation.

4.2.1. QUESTIONNAIRE DE MISE EN SITUATION

Le questionnaire de mise en situation permet, à partir de questions traitées lors de campagne de sensibilisation, de mesurer si l'apprenant a assimilé les messages qui lui ont été diffusés et si celui-ci les applique au quotidien.

Le but est pédagogique, une porte de sortie sera toujours insérée pour permettre une réponse

---

222 Société de formation anti-hameçonnage https://cybeready.com.

223 La sabermétrie ou sabermétrie (en anglais sabermetrics) est une approche statistique du baseball. Le mot tire son origine de l'acronyme SABR (pour Society for American Baseball Research) et fut suggéré par l'historien Bill James, l'un de ses adeptes les plus connus, qui décrit la sabermétrie comme « la recherche de la connaissance objective sur le baseball1 ». Source Wikipédia

« *honorable* » de la part de l'interlocuteur. Le choix de la porte de sortie « *honorable* » (exemple : je ne sais pas) sera considéré comme une non-assimilation de la mesure ou non compréhension ; dans ce cas, une nouvelle sensibilisation sera à mettre en œuvre.

Nous pouvons également utiliser ce questionnaire pour évaluer notre auditoire, avant la préparation de la campagne de sensibilisation afin de nous concentrer sur les sujets épineux.

Le questionnaire a été posté sur internet, entre le 8 juillet et le 10 novembre 2017, auprès de personnes, non professionnelles de la sécurité et des systèmes d'information et utilisant un ordinateur. Il y a eu 78 réponses, 9 réponses ont été éliminées de l'étude car elles étaient trop incomplètes (2 champs renseignés sur 94) (voir §2.4.4 page 73), donc 69 réponses exploitées.

QUELS APPAREILS (PROFESSIONNELS OU PERSONNELS) UTILISEZ-VOUS POUR VOTRE ACTIVITE PROFESSIONNELLE ?

L'usage des matériels professionnels 70 % est, globalement, supérieur à celui de matériel personnel 30 %.

EN DEPLACEMENT, QU'UTILISEZ-VOUS ?

Dans l'ensemble les utilisateurs sont « *raisonnables* ». L'usage de mobile personnel, dans les organisations publiques, est probablement dû aux coûts entraînés d'ordiphone et de l'abonnement.

QUE FAITES-VOUS LORSQUE VOUS ETES EN DEPLACEMENT PROFESSIONNEL ?

Les réponses étaient libres et des suggestions étaient indiquées dans l'intitulé de la question :

Les personnes en déplacement consultent leur courriel (76 % tout support confondu) et se connectent à leur organisation via un VPN[224] (48 %). Les usages suivants sont l'utilisation d'applications bureautiques (17 %) et le partage de document (14 % l'usage de Dropbox est supérieur au Cloud de l'organisation !).

AUTHENTIFICATION

- *Combien de mots de passes utilisez-vous dans notre activité professionnelle ?*
- *Comment gérez-vous vos mots de passe*
- *Avez-vous recours à d'autres systèmes d'authentification ?*

La direction du système d'information, des répondants, a pris conscience de l'importance de proposer des outils sécurisés pour stocker les mots de passe, ce qui permet d'en changer plus souvent, de les complexifier et d'en avoir un différent par application. Ces outils apportent du confort et de la sécurité aux acteurs de l'organisation et à la protection de l'information. Nous distinguons deux types de comportement dans les réponses : *à risques* et *sécurisés* :

	COMPORTEMENT	COMMENTAIRE
Comportements sécurisé	Nous avons entre 5 et 10 mots de passe ou plus	10 mots de passe sous-entendent que l'utilisateur accède à peu d'application ou site internet, dans le cas contraire, ce point sera considéré comme à risque.
	Vous utilisez un mot de passe différent pour chaque service / authentification / application	Les bonnes pratiques sont respectées.
	Nous avons une mémoire d'éléphant	Il est préférable de garder les mots de passe

[224] VPN : Virtual Private Network

	COMPORTEMENT	COMMENTAIRE
	pour retenir tous nos mots de passe	dans sa tête et non sur un post-it collé sur son écran d'ordinateur, par exemple !
	Il y a un logiciel installé sur notre ordinateur/matériel qui enregistre et gère tous vos mots de passe de manière sécurisée (keepass par exemple).	Ces outils apportent une sécurité et permettent d'utiliser des mots de passe complexes.
	Nous avons recours à un système d'authentification de type certificat personnel Token, authentification à double facteur, Biométrie (empreintes digitales, reconnaissance faciale).	Les clefs d'authentification se sont démocratisées et sont commercialisées auprès de grands distributeurs [225] pour un tarif allant de 10€ à 50€ environ. C'est une bonne alternative.
Comportement à risques	Nous avons un seul mot de passe pour tout service / authentification / application	Attention ! Si celui-ci est corrompu, l'accès à l'ensemble des données est possible. Ce plus le mot de passe est simple et cours, cela augmente le risque.
	Nous avons moins de 5 mots de passe	C'est peu, cela veut dire que le même mot de passe est utilisé pour plusieurs applications, cela revient à la réflexion précédente.
	Vous utilisez le même mot de passe pour des comptes personnels et professionnels	Tous les risques sont permis ! Cette attitude est un vrai jack pot pour les cybers criminels.
	Vous notez vos mots de passe sur des post-it (écran ou dos de l'ordinateur par exemple) ou sur une feuille au fond de notre tiroir.	Cela veut dire que, la personne qui nettoie notre bureau, nos collègues, nos clients, nos prestataires et toutes personnes de passage à potentiellement accès aux données de l'organisation !
	Vous notez vos mots de passe dans un carnet bien caché	
	Nous avons d'autres techniques/astuces : mots de passe écrits sur le tableau de notre bureau (malin ! Vous n'avez qu'à lever les yeux), tatouage, pyrogravure du bureau, encre sympathique, fausses notes, code Cesar, machine Enigma d'occasion…	Trêve de plaisanterie, les mots de passe doivent être enregistrés, sécurisés et facilement utilisables au quotidien.
	Vos mots de passe sont tous enregistrés dans un fichier sur notre ordinateur, vous n'avez qu'à ouvrir ce fichier (Word par ex) et copier le mot de passe et l'identifiant dont vous avez besoin (vous avez juste des problèmes pour retrouver le fichier).	Il existe des outils très simples sur internet pour déverrouiller un mot de passe d'un fichier Word, pire nous pouvons poster le fichier sur un site internet et celui-ci sera déverrouillé et téléchargeable. Excel est concerné également.
	Notre navigateur web stocke tous vos mots de passe	Le navigateur stocke les mots de passe sur l'ordinateur, sous qu'elle forme et cette sécurisation est-elle chiffrée ? Cette formule est à éviter tant que le cryptage n'est pas assuré. Un logiciel de gestion des mots de passe compatible avec les applications est préférable. Certains logiciels renseignent automatiquement les champs des applications, des sites internet…
	Vous utilisez un service en ligne gratuit	Un service est gratuit que pour celui qui

[225] voir https://www.amazon.fr/s/ref=nb_sb_ss_i_1_2/259-2389881-3033368?__mk_fr_FR=%C3%85M%C3%85%C5%BD%C3%95%C3%91&url=search-alias%3Delectronics&field-keywords=u2f&sprefix=U2%2Celectronics%2C887&crid=3QQDSXA94RQTF

	COMPORTEMENT	COMMENTAIRE
	pour enregistrer vos mots de passe	l'utilise ! Qui est derrière le site ? Comment sont protégées les données ?

COMBIEN DE PERSONNES CONNAISSENT NOTRE MOT DE PASSE ?

La grande majorité des personnes garde ses mots de passe secrets, même si parfois, aux grés des absences et des nécessités de service, les personnes viennent à partager leurs mots de passe avec une personne de confiance.

Ce comportement est risqué, il est important de comprendre pourquoi, les répondants donnent leurs mots de passe (pas de partage de messagerie ni de document via une GED ?) et d'y apporter une solution.

4.2.2. SCENARIOS D'INCIDENTS

Les scénarios sont une autre manière de mesurer la maturité de notre auditoire. « *L'histoire* » qui est racontée, met en situation la personne et est découpée en deux temps.

En premier, le décor est planté avec un enchaînement de catastrophes, amenant une réflexion sur l'impact sur l'activité professionnelle du répondant.

En deuxième point, les actions, que cette personne serait prête à accepter pour répondre à l'incident.

Ce mécanisme est subtil, dans le sens où nous alléchons l'interlocuteur, avec une histoire teintée d'humour, nous le sensibilisons en lui faisant prendre conscience des conséquences de ses actes et nous l'amenons à accepter des préconisations que nous lui aurions prodiguées, en fin de compte.

La personne sera plus encline à accepter des actions restrictives si elle participe la décision « à *l'insu de son plein gré* ».

Les mêmes personnes interrogées au §4.2.1 page 123, ont été questionnées sur la deuxième partie du scénario.

➔ SCENARIO D'INCIDENT 1 : CLEF USB

Sur le parc de stationnement, Nous avons trouvé une clé USB ! Quelle chance ! Hop, arrivé au bureau, vous la connectez pour éventuellement identifier le collègue qui l'aurait perdu, mais la clé semble vide.

Deux heures plus tard, votre ordinateur est inutilisable. La clé était piégée !

Pas de panique, l'assistance du service informatique est là pour vous aider, mais ils annoncent un délai de 3 jours pour vous remettre sur les rails.

Quel impact ce contretemps a-t-il sur votre activité métier ?

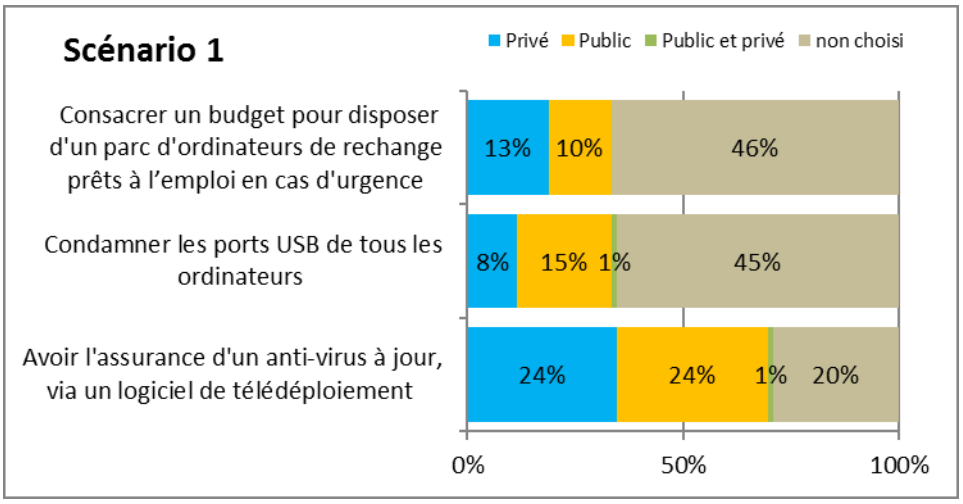
- Trois jours sans ordi, merci pour la cure de désintoxication
- Un tel retard va compromettre des travaux importants
- Un tel retard aura un impact sur le travail d'équipe
- C'en est trop… Je craque

Quelles mesures seriez-vous prêts à accepter pour que ce scénario ne se produise pas ?

- Condamner les ports USB de tous les ordinateurs
- Avoir l'assurance d'un antivirus à jour, via un logiciel de télé déploiement

- Consacrer un budget pour disposer d'un parc d'ordinateurs de rechange prêts à l'emploi en cas d'urgence.

ANALYSE DES REPONSES



ID n° 62 mise en situation, réponses au scénario 1

L'usage de la clef USB serait-il plus répandu et autorisé dans le domaine public que privé pour accepter de condamner les ports USB des ordinateurs ? Nous pouvons répondre par l'affirmation au vu de notre expérience dans le domaine hospitalier, nous ne connaissons pas les autres usages dans d'autres administrations.

Les utilisateurs font confiance à la protection d'un antivirus, lorsqu'il est déployé sur les postes. Attention à ce qu'il soit à jour ! Il est à noter que les antivirus sont mis à jour après la découverte de virus, que faire si le virus a déjà atteint le système d'information ? Les éditeurs proposent plusieurs parades pour analyser le comportement des ordinateurs et relever des actions anormales (exemple : minage – utilisation d'un ordinateur pour créer de la monnaie virtuelle comme le Bitcoin[226]- à l'insu de l'utilisateur, ou pic de l'usage du processeur de l'ordinateur anormal…).

Le test de « *l'abandon* » d'une clef USB dans un endroit visible de l'organisation, avec un logiciel de cryptage installé dessus est révélateur du comportement des acteurs de l'organisation. Les résultats pourront être utilisés en campagne de sensibilisation.

➔ *SCENARIO D'INCIDENT 2 : STAGIAIRE ET PERSONNEL INTERIMAIRE*

Notre dernier stagiaire a été recruté par une organisation qui développe des services fortement liés à vos domaines.

Êtes-vous sûr qu'il n'a plus accès à aucune donnée qui pourrait avantager vos concurrents ? À quelles données le stagiaire a-t-il pu accéder concernant l'ensemble des projets du laboratoire ?

- Cette question vous semble-t-elle préoccupante ?

---

226 Bitcoin est une cryptomonnaie autrement appelée monnaie cryptographique. Dans le cas de la dénomination unitaire, on l'écrit « bitcoin » et, dans le cas du système de paiement pair-à-pair on l'écrit « Bitcoin ». L'idée fut présentée pour la première fois en novembre 2008 par une personne, ou un groupe de personnes, sous le pseudonyme de Satoshi Nakamoto. Le code source de l'implémentation de référence fut quant à lui publié en 2009. Source Wikipédia.

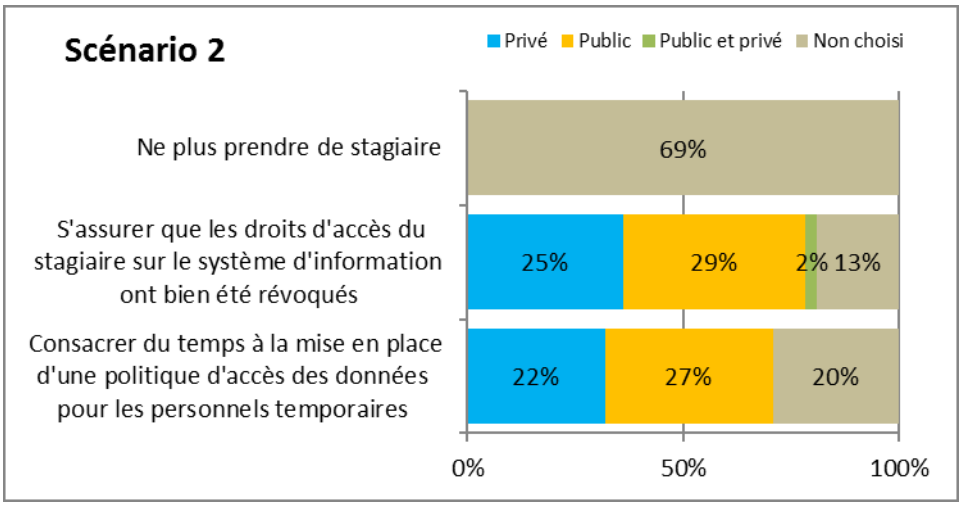
- Mes projets intéressent des industriels ? Tant mieux je leur donne tout avec le sourire !
- Bof, je ne vois pas ce qui peut intéresser la concurrence dans mes travaux.
- Mes travaux sont le fruit d'un long travail, je dois absolument vérifier qu'ils sont bien protégés (aller voir mon correspondant informatique).
- On est dans un cas d'espionnage industriel avéré avec des conséquences sur la valorisation de mes travaux. Je dois alerter quelqu'un !!!

Quelles mesures seriez-vous prêts à prendre pour éviter la fuite de vos travaux vers une activité concurrente ?

- Consacrer du temps à la mise en place d'une politique d'accès des données pour les personnels temporaires.
- S'assurer que les droits d'accès du stagiaire sur le système d'information ont bien été révoqués.

Ne plus prendre de stagiaire

ANALYSE DES REPONSES



ID n° 63 mise en situation, réponses au scénario 2

Les stagiaires sont appréciés, aucune réponse n'a été relevée, quant à ne plus accueillir ce genre de personnel dans les organisations.

Les deux autres questions, relèvent de la gestion des droits et des habilitations. C'est un sujet stratégique et récurrent des organisations.

Des outils de gestion des habilitations centralisés existent sur le marché (exemple : Ilex[227]). La première étape consistera à mettre en place une gouvernance des habilitations (qui a le droit de faire quoi, sur quoi et quand ou combien de temps)[228].

Certains logiciels intègrent cette gestion. C'est mieux que rien mais aucune harmonisation n'est mise en place en transverse et cela nécessite une mise à jour manuelle de chaque logiciel. Autant dire que les habilitations ne sont jamais à jour.

Les estimations générales indiquent que 80 % des données des organisations sont « non structurées », c'est-à-dire sans un format prédéfinit (serveurs de fichiers, courriels…). Il est

227 https://www.ilex-international.com/

228 Voir les recommandations de la CNIL https://www.cnil.fr/fr/securite-gerer-les-habilitations

indispensable de sécuriser ces informations afin d'éviter toute fuite ou compromission.

➔ SCENARIO D'INCIDENT 3 : ORDINATEUR VOLE, PERDU…

Au cours d'un déplacement professionnel, sur le chemin du retour, vous vous rendez compte que votre ordinateur portable a disparu. Votre dernière sauvegarde est très récente… Mais elle était sur le disque dur dans la même mallette et elle a aussi été volée. Votre ordinateur n'est pas chiffré, le voleur aura accès à toutes les données !

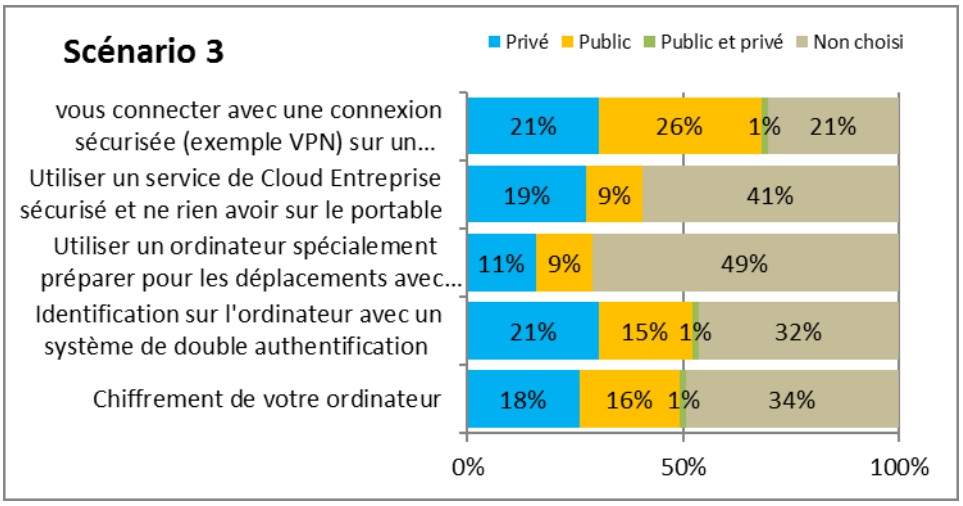
Avant de répondre à cette question, pensez aux éléments suivants :

- Votre navigateur sauvegarde vos mots de passes privés et professionnels ?
- Vos travaux ont-ils un aspect confidentiel ?
- Avez-vous des données personnelles sensibles sur votre ordinateur (RIB, scan de passeport, photos de famille) ?
- Savez-vous comment récupérer vos données de travail ?
- En combien de temps pouvez-vous vous remettre au travail à la suite de cet incident ?
- Quelle répercussion de ce vol pouvez-vous tolérer ?
- Le voleur a accès à mes données professionnelles
- Le voleur a accès à mes données personnelles
- Le voleur peut prendre mon identité sur tous les services en ligne
- Mes données sont perdues, 6 mois de travail à reprendre

Quelles mesures seriez-vous prêts à accepter pour éviter que le scénario précédent n'arrive ?

- Chiffrement de votre ordinateur,
- Identification sur l'ordinateur avec un système de double authentification,
- Utiliser un ordinateur spécialement préparer pour les déplacements avec le minimum d'applications pour travailler (ex : Word, Excel, PowerPoint),
- Utiliser un service de Cloud Entreprise sécurisé et ne rien avoir sur le portable,
- Vous connectez avec une connexion sécurisée (exemple VPN) sur un service en ligne sécurisé (exemple extranet) et ne rien avoir sur votre ordinateur,
- Autre.

ANALYSE DES REPONSES



ID n° 64 mise en situation, réponses au scénario 3

Les utilisateurs, ont conscience des risques qu'ils encourent avec leur matériel en déplacement. Ils

sont prêts à accepter des solutions sécurisées pour ce connecteur à leur organisation, afin d'avoir accès à leur environnement de travail et leurs documents.

Cette tendance se retrouve dans les réponses apportées au §4.2.1 *Que faites-vous lorsque vous êtes en déplacement professionnel ?* Page 123 quant à leur comportement en déplacement.

L'usage du VPN, de par notre expérience, est couramment utilisé. Le cloud computing[229] se développe et permet de proposer des outils en SAAS (software as a service[230]) comme la suite bureautique 365 de Microsoft ou des outils métiers comme les outils de l'éditeur SAGE (gestion comptable, finance, RH…). L'accès est sécurisé et aucune information ne transite sur l'ordinateur. L'utilisateur à toutefois le choix parfois de stocker de l'information sur son ordinateur, donc une réponse, comme le chiffrage de la machine pourra être apportée afin de protéger cette information.

➔ *SCENARIO D'INCIDENT 4 : USURPATION D'IDENTITE*

Vous vous rendez compte que votre identifiant et votre mot de passe ont été utilisés par quelqu'un d'autre que vous.

Le malfaiteur a pu l'utiliser pour accéder à divers services et applications en notre nom.

Quelle action mettriez-vous en place ?

- Faire porter un badge à tout le personnel
- Faire porter un badge à tous les visiteurs extérieurs
- Limiter les accès au bâtiment à une porte passant par l'accueil
- Contrôler l'accès aux copieurs (sous clé)
- Demander aux services de gestion des copieurs de désactiver les fonctionnalités à risque
- Autre :

Evaluez l'impact que cela aurait dans votre activité métier.

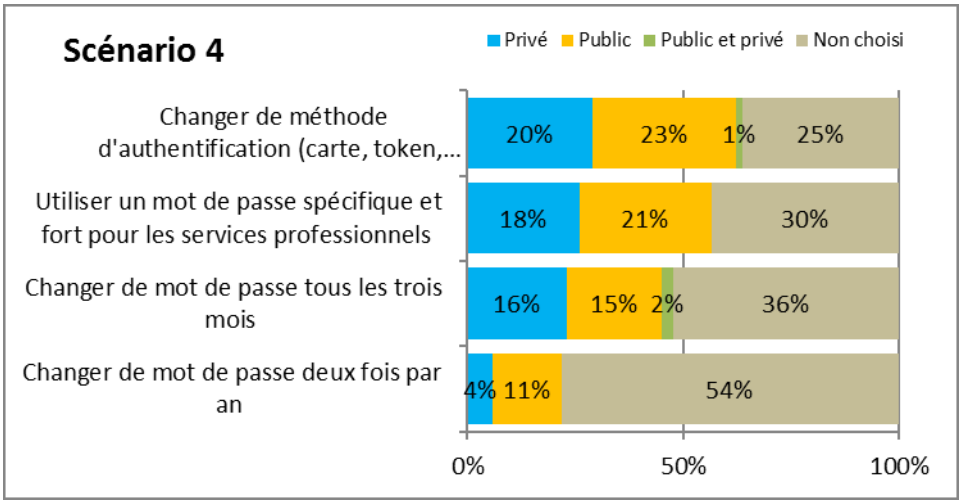
- Lire votre messagerie, envoyer des messages en votre nom.
- Accéder à vos espaces de stockage.
- Consulter votre dossier administratif (adresse, téléphone, carrière, avancement).
- Quelles mesures seriez-vous prêt à accepter pour limiter ce risque ?
- Utiliser un mot de passe spécifique et fort pour les services professionnels,
- Changer de mot de passe deux fois par an,
- Changer de méthode d'authentification,

---

229 Le cloud computing, en français « l'informatique en nuage » consiste à exploiter la puissance de calcul ou de stockage de serveurs informatiques distants par l'intermédiaire d'un réseau, généralement Internet.

230 Logiciels installés sur des serveurs distants plutôt que sur la machine de l'utilisateur. Les clients ne paient pas de licence mais un abonnement pour utiliser le produit.

ANALYSE DES REPONSES



ID n° 65 mise en situation, réponses au scénario 4

Nous notons la contradiction des réponses, après lecture du scénario, par rapport aux réponses apportées au §4.2.1 Authentification page 124.

Les répondants sont prêts à accepter de fortes contraintes sur la gestion de leur authentification, alors que 23 % du personnel public et 19 % des personnels privés ont un comportement à risque.

Nous pouvons peut-être en déduire que la mise en situation permet de réaliser le danger que l'on fait courir à l'organisation, si nous ne changeons pas le mot de passe ou ne nous plions pas aux bonnes pratiques. Ce point est à retenir dans le cadre de la campagne de sensibilisation : apporter des scénarios dans lesquels l'acteur pourra se projeter pour comprendre la conséquence de ses actes.

➔ *SCENARIO D'INCIDENT 5 : VIRUS*

Un collègue a été infecté par un cryptovirus. Celui-ci chiffre toutes les données.

Notamment, des données sur le serveur centralisé auxquelles, vous avez besoin d'accéder, sont devenues complètement inutilisables. Vous avez contacté l'assistance informatique qui s'efforce de remettre le service en état mais cela prendra du temps, environ 3 jours de travail, et les sauvegardes datent de 2 jours.

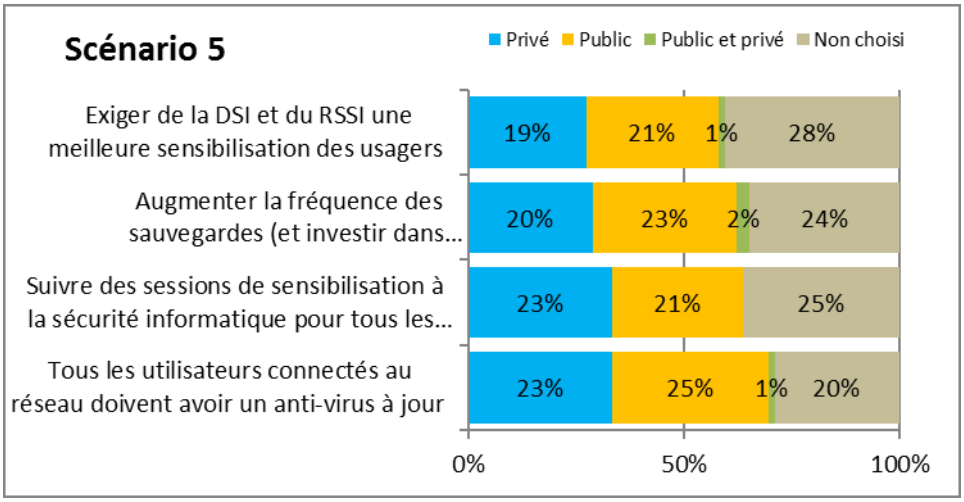
Evaluez l'impact de ce contretemps sur votre activité métier.

- Je perds du temps et des journées de travail, ce n'est pas trop grave,
- 3 jours de délais ! Ça me met encore plus en retard, je n'avais pas besoin de ça !
- Je rate une échéance importante, cet incident est catastrophique pour moi,
- C'est une catastrophe pour l'ensemble du travail d'équipe.

Quelles mesures, pensez-vous raisonnable de prendre, pour éviter ce scénario ?

- Tous les utilisateurs connectés au réseau doivent avoir un antivirus à jour,
- Suivre des sessions de sensibilisation à la sécurité des informations pour tous les usagers,
- Augmenter la fréquence des sauvegardes et investir dans l'infrastructure nécessaire,
- Exiger de la DSI et du RSSI une meilleure sensibilisation des acteurs de l'organisation

ANALYSE DES REPONSES



ID n° 66 mise en situation, réponses au scénario 5

Les acteurs se reposent sur la technique pour se protéger à 94 % ; les réponses sont logiques vu que les répondants affirment ne pas avoir suivi de formation ou de campagne de sensibilisation dans leur organisation (voir les résultats de l'enquête §2.4.4 page 73).

Nous pouvons en conclure que les utilisateurs sont conscients que des actions de sensibilisation sont nécessaires (85 % des réponses), pour éviter ou, au moins diminuer, l'arrivée de ce genre de scénario catastrophe. La conduite du changement se fera d'autant mieux avec des acteurs motivés et conscients des dangers.

4.2.3. COMPARAISON ENTRE LES REPONSES DES PROFESSIONNELS DE LA SECURITE ET LES ACTEURS DE L'ORGANISATION

➔ *LA SENSIBILISATION A LA SECURITE DANS VOTRE ENTREPRISE SE PRESENTE SOUS QU'ELLES (S) FORME (S) ?*

La même question a été posée aux professionnels de la protection de l'information et, aux acteurs de l'organisation, non professionnels des systèmes d'information.

Nous notons des réponses très éloignées entre les « *deux camps* ».

Dans le tableau ci-dessous regroupant les résultats aux questions posées, on peut voir que d'un côté des actions sont entreprises (A), comme l'envoi de courriels ciblés, et de l'autre côté (B) le message n'est pas reçu, car celui-ci n'est pas lu ou, interprété comme tel.

La même réflexion se pose sur l'intranet, outils de diffusion de l'information, auprès de l'ensemble des acteurs de l'entreprise. (A) publie de l'information (75 % et 72 %) mais (B) ne le voit pas ou, ne le lit pas (41 % et 54 %).

Les deux secteurs sont en adéquation sur les supports utilisés, comme les formations en présentiel et le bulletin d'information de sécurité.

	A PROFESSIONNELS DE LA SECURITE		B ACTEURS DE L'ORGANISATION		
TYPE DE SUPPORT	PRIVE	PUBLIQUE	PRIVE	PUBLIQUE	PUBLIC ET PRIVE
Courriels ciblés	74 %	83 %	38 %	60 %	2 %
Intranet	75 %	72 %	41 %	54 %	5 %
Réunions	66 %	73 %	60 %	40 %	0 %
Formation des utilisateurs en présentiel	47 %	65 %	43 %	57 %	0 %
Documentation	42 %	43 %	60 %	40 %	0 %
Séminaire d'entrée	32 %	45 %	67 %	33 %	0 %
Campagnes de courriels phishing	41 %	35 %	100 %	0 %	0 %
Rendez-vous en face-à-face	27 %	35 %	100 %	0 %	0 %
Bulletin d'information sécurité	32 %	23 %	37 %	58 %	5 %
Formation en ligne	44 %	12 %	75 %	25 %	0 %
Serious Game génériques	16 %	8 %			
Serious Game adaptés	13 %	7 %	0 %	100 %	0 %

ID n° 67 support de la sensibilisation en entreprise

En conclusion : une analyse des campagnes de sensibilisation mises en œuvre est nécessaire car, la perception est parfois, en complète opposition, sur certains sujets comme nous le constatons ci-dessus.

4.3. COUT DE LA SENSIBILISATION

En l'espace d'un an et, malgré une actualité forte et anxiogène, la cyber sécurité est passée de la première à la cinquième place des priorités des organisations, selon l'enquête annuelle « *Building Trust* »[231] de KPMG. En 2016, 83 % des PDG avaient indiqué que la réduction des risques cyber faisait partie de leur rôle. Ils ne sont plus que 72 % à l'affirmer en 2017 !

> *« La sensibilisation peut coûter des centaines de milliers d'euros » Guillaume Laudière, consultant sécurité chez Devoteam*[232].

Le responsable de la mise en place d'une campagne de sensibilisation est, généralement, le Responsable de la Sécurité du Système d'Information (RSSI), de l'organisation.

L'appui du commanditaire est nécessaire au RSSI pour mener à bien sa mission, comme dans tout projet. Il pourra s'appuyer sur les services supports de l'organisation, pour diminuer les coûts, comme le service de formation interne, les ressources humaines, le service de communication, le service de reprographie, etc. Ou faire appel à sa créativité, s'il est seul ou, a peu de moyens !

YouTube regorge de vidéo de sensibilisation. L'ANSSI met des supports à disposition gratuitement sur son site. On peut, également s'appuyer sur les MOOC *Secnumacademie*[233] et les outils mis à

231 Source http://itsocial.fr/metiers/direction-generale/pdg-ont-chemin-a-faire-de-prendre-cybersecurite-serieux/

232 Devoteam est une entreprise de services du numérique (ESN) française spécialisée dans le conseil en IT, sécurité, cloud computing et big data.

233 MOOC Secnumacademie https://secnumacademie.gouv.fr/

disposition pour le mois de la cyber sécurité (en octobre)[234].

Nos amis francophones, canadiens et suisses, ont commencé ce genre d'actions, il y a plusieurs années et partagent leurs supports sur internet[235].

Les RSSI ont un budget limité, et malheureusement, la sensibilisation vient souvent en dernier. Donc, lorsqu'on évalue le budget d'une campagne entre 30 000 € et plusieurs milliers d'euros, suivant le type et la taille de l'organisation, les actions entreprises sont basiques, afin de rentrer dans les enveloppes allouées.

Par ailleurs, le RSSI est souvent seul, donc son temps est compté pour mettre en œuvre des campagnes complexes ou basées sur un large panel d'outils. Il va se replier sur des sessions de formation en ligne, des courriels ponctuels et des messages diffusés sur l'intranet.

Selon une étude du cabinet Wavestone (§2.4.5 page 75) pour la société Carmignac (§2.4.6 page 77), les prix varient, selon les prestataires et supports proposés :

TYPE	SOCIETE	OUTILS	COUT	PERSONNALISATION
Serious game	Mavi interactive	Modules SSI réutilisables	Moyen (~10K€ + coût de personnalisation si nécessaire)	Faible
	Œil pour œil gamification	Jeux adaptés au contexte, à créer de bout en bout	Elevé (30K€ à 50K€ pour 30 minutes de modules)	Forte
Saynètes avec questionnaire	Conscio technologie	Modules « protection des données » et « Sécurité SI » réutilisables	Moyen (~10K€ pour 2 modules)	Faible
Diapositives avec questionnaire	Elucidat Beedeez	Diapositives suivies de questionnaires, sur web ou ordiphone	Moyen	Forte
Formation en ligne spécial santé	Pour les adhérents à la centrale d'achat CAIH réservé aux hôpitaux	Module adapté à la santé	Pour un seul marché de 0,40 € HT par lit de l'établissement, avec un plafond annuel de 1 000,00 € HT.	

ID n° 68 choix de prestataires. Source Wavestone

À cela les coûts de licence s'additionnent (exemple : pour un logiciel de formation en ligne installé en local ou utilisé en SAAS), la mobilisation des personnes formées, le nombre de jours de formation, par une personne interne ou externe, dans ce cas le prix horaire de la prestation est d'autant majoré :

TYPE	CHARGES ANNEE 1	CHARGES ANNEES SUIVANTES
Tous les collaborateurs (~ 300 personnes)	31 J.H. + 10 000 € 20 minutes par participant, soit	18 J.H. + 10 000 € 20 minutes par participant, soit

234 https://www.ssi.gouv.fr/agence/cybersecurite/mois-de-la-cybersecurite-2018/

235 https://www.cse-cst.gc.ca/fr/its-interactive-gallery, https://security.web.cern.ch/security/training/fr/posters.shtml

TYPE	CHARGES ANNEE 1	CHARGES ANNEES SUIVANTES
	100 heures au total	100 heures au total
Top Management & Secrétariat général (~ 20 personnes)	5 J.H. 40 minutes par participant, soit 13 heures au total	2,5 J.H. 20 minutes par participant, soit 7 heures au total
Métiers sensibles (~ 100 personnes)	7 J.H.	1 J.H.
Comptabilité (~ 10 personnes)	3 J.H. Une heure par participant, soit 10 heures au total	3 J.H. Une heure par participant, soit 10 heures au total
Office Management (~ 5 personnes)	2 J.H. Une heure par participant, soit 5 heures au total	2 J.H. Une heure par participant, soit 5 heures au total
Commerciaux (~ 80 personnes)	Déjà comptabilisé dans « tous les collaborateurs - E-learning »	
Acteurs du PCA (~ 50 personnes)	24 J.H. 4 heures par participant, soit 200 heures au total	22 J.H. 4 heures par participant, soit 200 heures au total
Core Technologies (30 personnes)	5 J.H. Une heure par participant, soit 30 heures au total	0,5 J.H. Une heure par participant, soit 30 heures au total
TOTAL	**77 J.H. + 10 000 € 350 heures pour les participants, soit un peu plus d'une heure en moyenne par participant**	**93,4 J.H. + 10 000 € 350 heures pour les participants, soit un peu plus d'une heure en moyenne par participant**

ID n° 69 évaluation des coûts de la sensibilisation. Source Wavestone.

Une étude est à mener afin de prendre en compte la rentabilité de chaque action, afin d'établir un budget entre la fréquence, le coût et l'efficacité du support utilisé (ROI) :

ACTIONS	MESSAGES PRINCIPAUX	FORMAT	FREQUENCE	COUT	EFFICACITE
Formation En Ligne	Bonnes pratiques à adopter & règles de sécurité Enjeux de la protection des documents / données	Formation en ligne (20 minutes en ~4 modules)	Annuelle	Moyen à Elevé	Moyenne à Forte
Campagne de communication	Bonnes pratiques de sécurité, en lien avec les actualités (WannaCry, Petya, GDPR, etc.)	Courriel Impressions Ecrans	Mensuelle	Faible	Moyenne
Communication de la charte d'utilisation des moyens informatiques	Bonnes pratiques à adopter & règles de sécurité Enjeux de la protection des documents / données	Courriel	À l'initialisation et pour les nouveaux arrivants	Faible	Faible

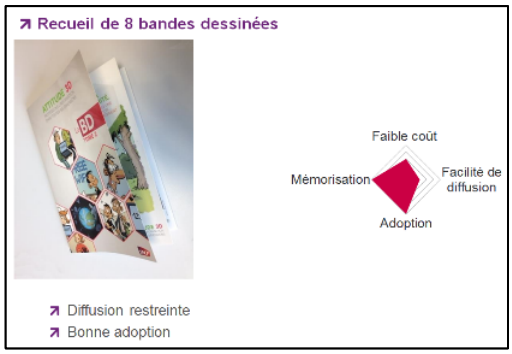
ID n° 70 ROI prestation / résultats attendus. Source Wavestone.

Les actions nécessaires pour mettre la campagne en place, sont également à considérer (Source Wavestone J.H. = Jour homme) :

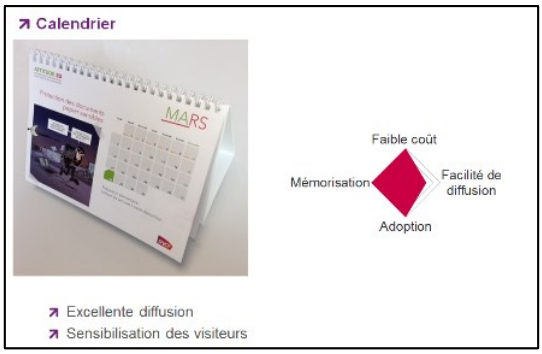
- **Charges de BUILD**
  - Choix de l'outil de formation en ligne ..... 3 J.H.
  - Personnalisation des modules ..... 5 J.H.
  - Validation et communication de la charte ..... 5 J.H.
- **Charges de RUN**
  - Licences pour l'outil de formation en ligne ..... 10K€ / an

- Pilotage de la campagne de formation en ligne ..... 5 J.H.
- Formalisation des supports de communication mensuels (campagne) .....1 J.H. / mois
- Communication de la charte ..... 1 J.H.

Certains supports ont un retour sur investissement intéressant et d'autres moins. La SNCF a réalisé une étude sur quatre axes, pour déterminer son budget annuel, par rapport à ses cibles :



ID n° 71 ROI des supports analysé chez SNCF



ID n° 72 ROI de la SNCF sur les supports diffusés.

4.4. COUT D'UNE NON SECURISATION

Le coût de la non-sécurisation peut être comparé à un iceberg :

- Dans la partie visible les dégâts sont directement mesurables, comme les pertes techniques (rachat d'un serveur, de matériels, honoraire d'avocat, enquêtes, audits, l'immobilisation des personnes qui ne peuvent plus travailler etc.).
- La partie cachée a un coût peu connu, car les entreprises ne révèlent pas ce genre d'information, ou parfois n'en ont pas conscience (voir Les 14 impacts d'une cyberattaque Annexe n°23 page 212).

Des coûts sournois se révèlent, comme :

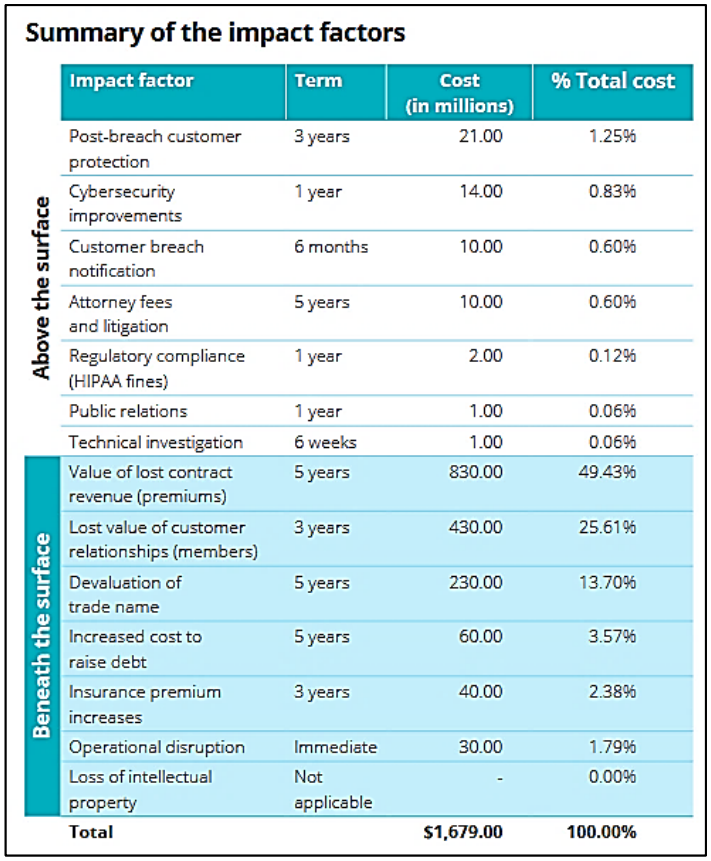
- La perte de confiance des clients (perte de chiffre d'affaires),
- L'augmentation des primes d'assurances,
- Le pillage intellectuel de brevet qui arrive sur des marchés parallèles,
- La perturbation de l'activité de l'organisation due, au temps de remise en route, au « retour nominal » et au temps de refonte des processus de l'organisation, etc.

La perte immatérielle représente plus de 40 % des dommages subis.

La gestion des premiers dommages sur l'organisation, représente moins de 10 % du coût global.

Ci-dessous un exemple d'étude réalisée par Deloitte Cyberattaques « *Comment chiffrer les impacts ? Le visible et l'invisible* » [236] Il est détaillé le cas d'un établissement de santé américain et une entreprise technologique, sur les dépenses engendrées à la suite d'une cyberattaque :

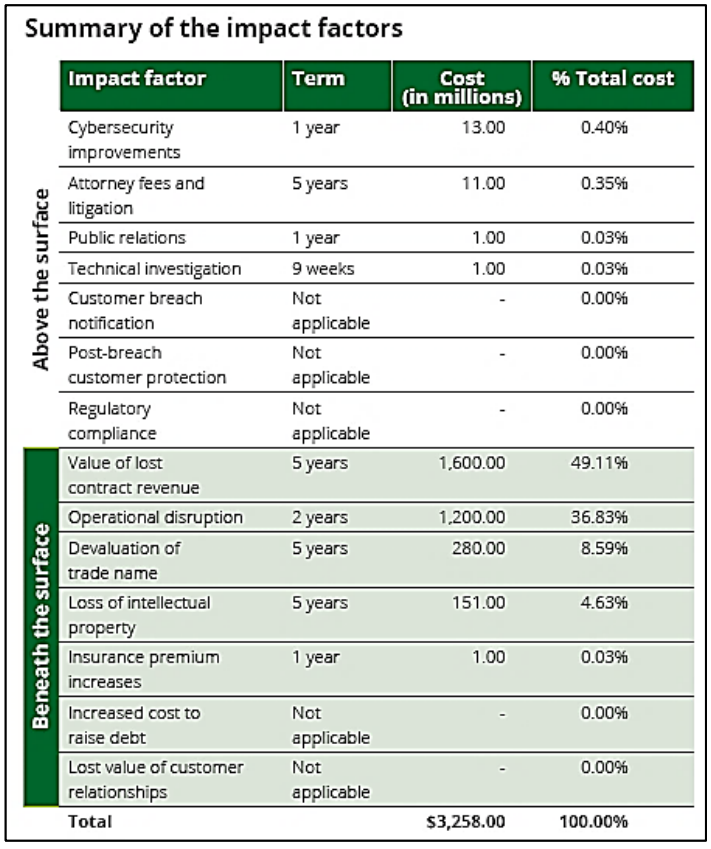
[236] source https://www2.deloitte.com/fr/fr/pages/risque-compliance-et-controle-interne/articles/cyberattaques-chiffrer-les-impacts.html



Summary of the impact factors

	Impact factor	Term	Cost (in millions)	% Total cost
Above the surface	Post-breach customer protection	3 years	21.00	1.25%
	Cybersecurity improvements	1 year	14.00	0.83%
	Customer breach notification	6 months	10.00	0.60%
	Attorney fees and litigation	5 years	10.00	0.60%
	Regulatory compliance (HIPAA fines)	1 year	2.00	0.12%
	Public relations	1 year	1.00	0.06%
	Technical investigation	6 weeks	1.00	0.06%
Beneath the surface	Value of lost contract revenue (premiums)	5 years	830.00	49.43%
	Lost value of customer relationships (members)	3 years	430.00	25.61%
	Devaluation of trade name	5 years	230.00	13.70%
	Increased cost to raise debt	5 years	60.00	3.57%
	Insurance premium increases	3 years	40.00	2.38%
	Operational disruption	Immediate	30.00	1.79%
	Loss of intellectual property	Not applicable	-	0.00%
	Total		**$1,679.00**	**100.00%**

ID n° 73 étude Deloitte Cyberattaques : comment chiffrer les impacts ? Le visible et l'invisible



Summary of the impact factors

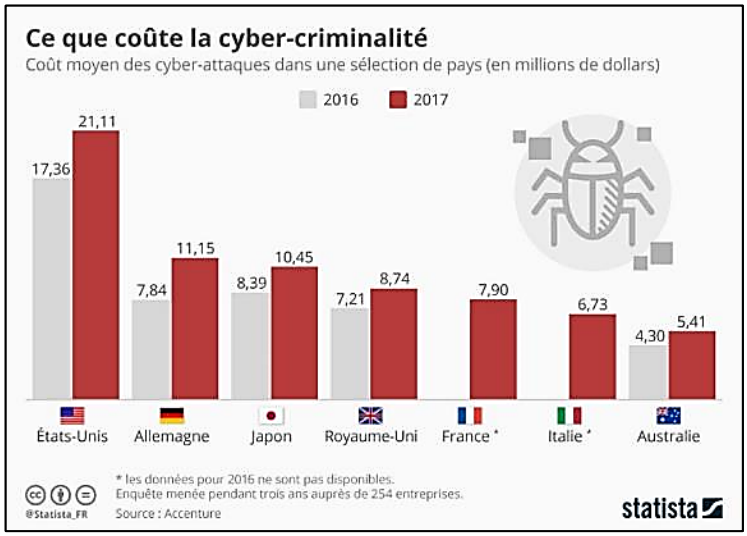
	Impact factor	Term	Cost (in millions)	% Total cost
Above the surface	Cybersecurity improvements	1 year	13.00	0.40%
	Attorney fees and litigation	5 years	11.00	0.35%
	Public relations	1 year	1.00	0.03%
	Technical investigation	9 weeks	1.00	0.03%
	Customer breach notification	Not applicable	-	0.00%
	Post-breach customer protection	Not applicable	-	0.00%
	Regulatory compliance	Not applicable	-	0.00%
Beneath the surface	Value of lost contract revenue	5 years	1,600.00	49.11%
	Operational disruption	2 years	1,200.00	36.83%
	Devaluation of trade name	5 years	280.00	8.59%
	Loss of intellectual property	5 years	151.00	4.63%
	Insurance premium increases	1 year	1.00	0.03%
	Increased cost to raise debt	Not applicable	-	0.00%
	Lost value of customer relationships	Not applicable	-	0.00%
	Total		**$3,258.00**	**100.00%**

ID n° 74 étude Deloitte Cyberattaques : comment chiffrer les impacts ? Le visible et l'invisible

Les dépenses, liées à des incidents de sécurité sont 76 % moins importants pour les organisations qui ont mené des campagnes de sensibilisation.

Moins de 5 % des entreprises françaises (6 % des particuliers) ont souscrit une cyber assurance en 2015[237].

Les organisations françaises ont investi, 4,3 millions d'euros, dans le renforcement de la sécurisation de leur système d'information, soit 10,2 % de plus qu'en 2016. Malgré ces efforts, celles-ci ont enregistré des pertes financières estimées à 2,25 millions d'euros, en moyenne, pour 4 550 tentatives d'instruction. Le montant des pertes financières est en hausse pour un nombre d'incidents similaires[238].



ID n° 75 coût de la cybercriminalité - Accenture

La cybercriminalité se porte bien !

L'étude « *Cost of cyber crime study 2017 insights on the security investments that make a difference* »[239] menée, auprès de 2000 spécialistes de la sécurité du système d'information de 254 entreprises dans le monde, indique que les cyberattaques ont un impact de plus en plus conséquent sur les organisations.

Le système d'information est au cœur des organisations de toute taille, un nombre de plus en plus grand d'information est digitalisé, par conséquent celles-ci subissent des attaques qui sont plus impactantes au vu des dégâts occasionnés. L'impact sera moins coûteux pour une petite entreprise mais aussi paralysant (exemple : système comptable crypté, campagne de phishing après le vol du fichier clients, fausse factures émises ou bon de commandes, etc.).

Les entreprises de plus petites tailles manquent de maturité en ce qui concerne la sécurité et de fait ne détectent pas toutes les attaques.

---

237 Source l'étude du cabinet d'audit et de conseil PwC « Le marché de la cyber-assurance : la Révolution commence maintenant »

238 Source PwC: « The Global State of Information Security® Survey 2018 »

239 Source Accenture "Cost of cyber crime study 2017 insights on the security investments that make a difference" : https://www.accenture.com/t20171006t095146z__w__/us-en/_acnmedia/pdf-62/accenture-2017costcybercrime-us-final.pdf%20-%20zoom=50

Plus l'organisation est grande et plus les coûts sont élevés :

TABLE 1 Quartile analysis	FY 2017	FY 2016	FY 2015	FY 2014	FY 2013
Cost expressed in US$	(n=254)	(n=237)	(n=252)	(n=257)	(n=234)
Quartile 1 (smallest)	$3,556,300	$3,477,633	$3,279,376	$2,967,723	$2,965,464
Quartile 2	$5,685,633	$5,567,110	$5,246,519	$5,107,532	$4,453,688
Quartile 3	$10,125,414	$9,854,250	$8,987,450	$8,321,024	$6,659,478
Quartile 4 (largest)	$16,852,250	$14,589,120	$13,372,861	$13,805,529	$14,707,980

ID n° 76 Accenture « Cost of cyber crime study 2017 insights on the security investments that make a difference » coût suivant la taille de l'organisation

Par ailleurs, les petites organisations de type PMI, PME, TPE pensent être moins attractives pour les pirates informatiques que les grandes entreprises ; ce constat est faux, car celles-ci sont souvent liées à d'autres organisations par des contrats de sous-traitance ou de fourniture de produits, donc elles subiront par répercussion ce genre de malveillance.

Le cyber terrorisme touche l'ensemble des entreprises, quelle que soit sa taille, les cybers attaquants font « feu de tout bois ».

Certaines organisations ont pris conscience de l'importance de protéger leur information, mais ce n'est pas le cas de toutes les entreprises qui alloue des budgets en deçà des préconisations (le syntec numérique préconise 5 à 20 % du budget SI).

Le « virage numérique » pousse les organisations vers le Cloud, la présence sur les supports mobiles, qui engendre d'autres risques, pas toujours maîtrisés car souvent déportés sur des prestataires externes.

Des campagnes de sensibilisations sont nécessaires dans les écoles de commerce en direction des futurs chefs d'entreprise et dans les chambres de commerce auprès des créateurs de PME, PMI et TPE.

Le coût moyen des cyberattaques se monte à 21 millions de dollars aux états Unis. En Europe, l'Allemagne enregistre la plus forte hausse de dépenses engendrées par ces attaques, passant de 7,84 à 11,15 millions de dollars entre 2016 et 2017 et en France ce coût est de presque 8 millions de dollars en 2017.

De manière générale le coût annuel moyen des secteurs les plus impactés est pour les banques et assurances de 18,28 millions de dollars et de 17,20 millions de dollars pour les entreprises liées à l'énergie [240].

Le pourcentage de coût des attaques est différent suivant les pays : l'Allemagne et L'Australie ont les attaques les par malware les plus coûteuses (23 % chacun), la France a les attaques Web les plus coûteuses (20 %) et l'Allemagne et le Royaume-Uni ont les attaques de déni de service les

[240] Source www.accenture.com

plus coûteuses (les deux 15 %).

Les coûts augmentent avec la fréquence des attaques, alors que l'on pourrait penser qu'une entreprise qui a été victime d'une cyberattaque, mettra tout en œuvre pour se protéger.

Kaspersky, a étudié les coûts provoqués par les erreurs humaines auprès de ses clients (80 % des incidents) : les grandes entreprises dépensent, en moyenne 551 000 $ pour se relever d'une cyberattaque, et 38 000 $ pour les PME.

Les attaques de phishing coûtent aux organisations jusqu'à 400 $ par employé et par an.

IBM Security et Ponemon Institute [241] ont publié leur huitième étude sur les coûts dus aux cyberattaques. 205 entreprises françaises se sont associées à l'étude au cours des huit dernières années et 32 entreprises ont participé à l'étude de 2017 réparties sur 13 secteurs économiques. Les informations relevées, sont des coûts réels et l'analyse a été effectuée sur 10 mois.

Le coût moyen par personne de la violation de données est passé de 141 euros en 2016 à 136 euros en 2017 et le coût total moyen pour les entreprises est passé de 3,40 millions euros en 2016 à 3,26 millions euros.

Le nombre d'enregistrements compromis, par attaque, variait de 5 150 à 74 000 et le nombre moyen d'enregistrements piratés était de 24 211.

Le nombre d'enregistrements compromis ainsi que les délais de découverte de la faille de sécurité influent sur les coûts.

Le délai d'identification d'une fuite d'information, par les organisations interrogées est passé de 201 jours en 2016 à 191 jours en 2017. Le nombre jours moyens pour contenir cette fuite était de 70 jours en 2016 et 66 jours en 2017.

Nous attribuons ces améliorations, aux investissements dans des technologies de sécurité, telles que l'analyse, le SIEM[242] (*security information and event management*), le cryptage à l'échelle de l'entreprise et les plates-formes de renseignements sur les menaces.

Bien qu'une certaine complexité, dans l'architecture du système d'information, soit censée faire face aux nombreuses menaces, auxquelles sont confrontées les organisations, une trop grande complexité peut avoir un impact sur la capacité à répondre aux attaques.

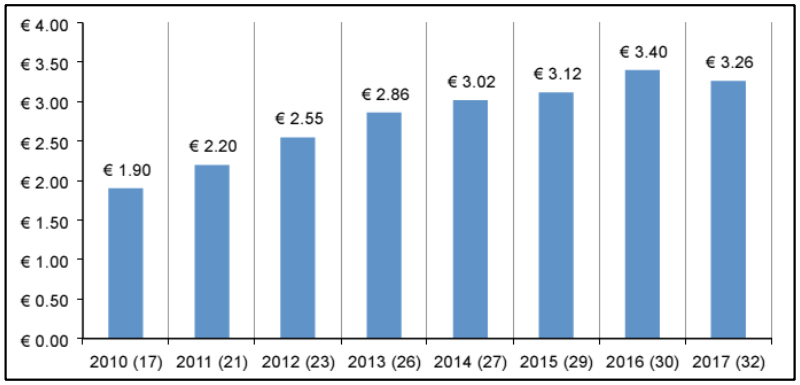
Les technologies disruptives, l'accès aux applications et aux données basées sur le Cloud, ainsi que l'utilisation des appareils mobiles (y compris BYOD et les applications mobiles) augmentent la complexité du traitement des risques de sécurité informatique et, des violations de données.

---

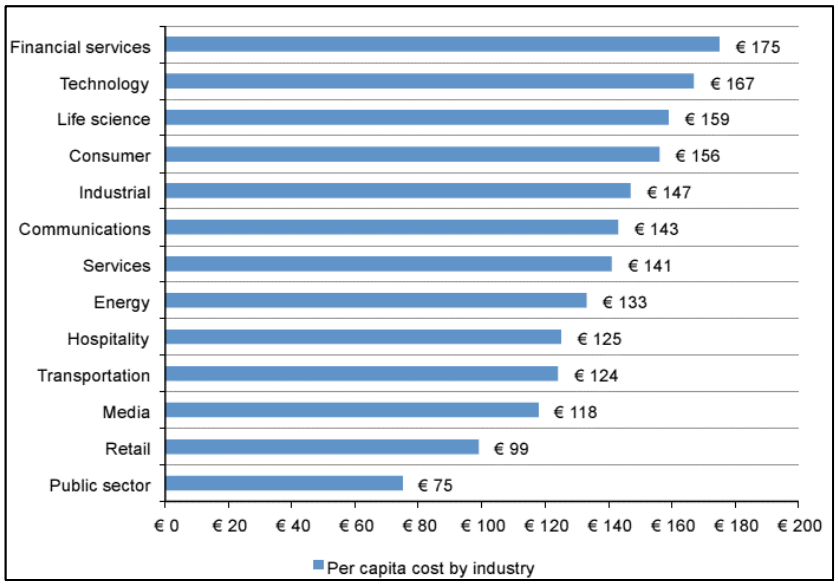
241 2017 Ponemon Cost of Data Breach Study: https://www.ibm.com/security/data-breach

242 Le principe du *security information management* (SIM) est de gérer les évènements du système d'information (SI). Appelés également SEM (*security event management*) ou SEIM (*security event information management*) ou encore SIEM (*security information and event management*), ils permettent de gérer et corréler les logs. On parle de corrélation car ces solutions sont munies de moteurs de corrélation qui permettent de relier plusieurs évènements à une même cause.

Près de la moitié des organisations représentées dans cette enquête (47 %), ont identifié et attribué, l'origine de la fuite d'information à une attaque malveillante ou criminelle. Nous pourrions en déduire que l'autre moitié est due à un facteur humain interne à l'organisation, à une défaillance de la gestion de la sécurité et de la protection de l'information (prestataires indélicats, ancien employé remercié…) ? Ce point n'est pas développé dans l'enquête.



ID n° 77 Le coût total moyen du piratage par organisation au cours des huit dernières années.

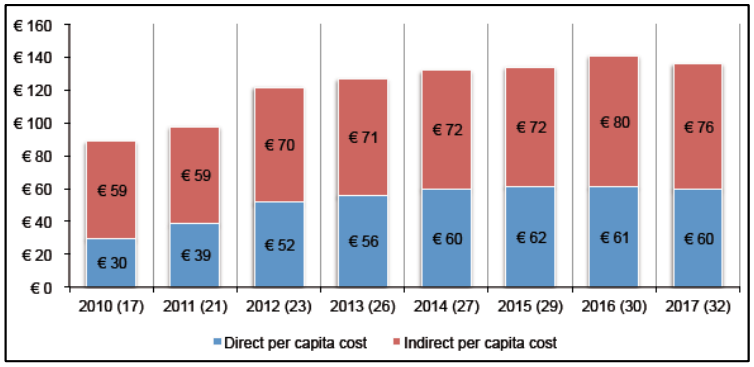


ID n° 78 coût par secteur économique

Certains secteurs, comme la banque ou les entreprises de pointe ont des coûts plus élevés que les autres secteurs.

Le coût des cyberattaques ramené par habitant a légèrement diminué

Les coûts indirects, comprennent l'organisation nécessaire à la résolution de l'incident et, les coûts directs sont des dépenses concrètes, comme l'achat d'un logiciel ou la prestation d'un spécialiste.



ID n° 79 Tendances des coûts directs et indirects de violation de données par habitant au cours des huit dernières années.

Des plateformes mettent à disposition des calculettes pour mesurer l'estimation des coûts d'un incident de sécurité :

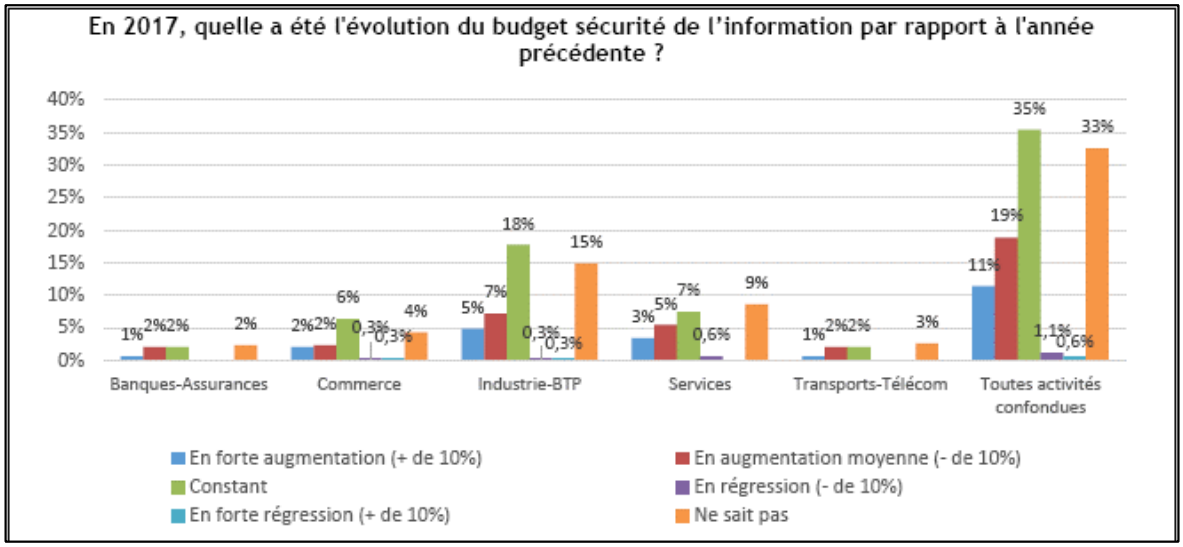
- Splunk :https://www.splunk.com/fr_fr/form/critical-it-incident-calculator.html
- Kaspersky : https://calculator.kaspersky.com/fr

4.5. BUDGET CONSACRE À LA PROTECTION DE L'INFORMATION

Le CLUSIF effectue une enquête approfondie tous les deux ans sur des secteurs d'activité privée et publique.

Globalement, nous constatons que le budget sécurité augmente dans les organisations privées, même si 33 % des personnes interviewées ne connaissent pas l'évolution du budget sur ce point ! Et que seulement 20 % des entreprises identifient les coûts liés à la sécurité de la protection de l'information.

Lorsque nous analysons les postes d'investissement, les solutions techniques ont la part belle avec 23 % du budget consacré à la « mise en place de solutions » et seulement 12 % sont alloués aux campagnes de sensibilisation.



ID n° 80 – évolution du budget sécurité selon les secteurs d'activité. En 2016, l'étude menée par Symantec met en évidence que seulement 6 % du budget total dédié aux services informatiques serait consacré à la sécurisation des systèmes.

Les organisations publiques, comme les établissements de santé, sont incapables d'identifier les coûts liés à la protection de l'information (80° %), et il est impossible d'identifier, de manière

factuelle le budget moyen consacré à la sécurisation de l'information. Comme dans le privé, le budget augmente par rapport à l'année précédente, mais celui-ci est mal identifié car les établissements de santé n'arrivent pas à corréler les coûts par rapport à la sécurité. Les infrastructures sont renforcées par la mise en place de solutions techniques (25 %), comme dans le privé.

Les établissements de santé se positionnent au même niveau d'investissement pour la que les organisations privées, en consacrant 11 % du budget sécurisation à la sensibilisation des acteurs de l'organisation.

4.6. CONCLUSION

Il est indispensable d'intégrer la cyber sécurité à tout processus de traitement des données afin d'en assurer la protection de façon optimale.

Nous devons intégrer la sécurité de l'information à chaque étape du traitement des données

Les coûts de la mise en œuvre de la sécurité de l'information peuvent être contrôlés et organisés, contrairement aux coûts élevés des incidents de sécurité (voir §4.4 page 136).

L'information est une ressource critique de l'organisation et sera traitée comme tout autre actif (voir De quelle information parlons-nous ? page 8), donc une stratégie de gouvernance de la cybersécurité sera mise en place qui traitera, aussi, du budget à affecter à la protection de l'information.

Un arbitrage entre efficacité et efficience sera à discuter et un point d'équilibre à trouver. Ceci n'est pas évident car les coûts d'éventuelles attaques sont à identifier et les impacts ne sont jamais connus avec certitudes (iceberg).

L'information est essentielle à l'ensemble des métiers et support de l'organisation, celle-ci est largement digitalisée, partagée en interne ou en externe (Cloud), la protection de l'information affecte donc l'ensemble de l'organisation.

Lorsque nous regardons l'investissement nécessaire à la protection par rapport aux coûts connus, immédiats et à moyen et long terme d'une cyberattaque, « jouer les autruches » est irresponsable pour la réussite et la pérennisation de l'organisation.

Une organisation est surtout constituée d'êtres humains sans lesquelles elle ne pourrait pas fonctionner. Mettre en danger l'entreprise revient aussi à mettre en danger les personnes qui y travaillent et qui contribue à sa richesse et par répercussion d'autres partenaires (sous-traitants, fournisseurs…).

Ces mêmes êtres humains qui ont un minimum de conscience vis-à-vis des malveillances en provenance d'internet, adoptent des comportements à risque par méconnaissance des dangers (voir §4.2.1 page 123) qu'ils font peser sur l'organisation ou qu'ils encourent dans leur vie personnelle.

Les acteurs de l'entreprise sont prêts à accepter des contraintes du moment que ceux-ci comprennent pourquoi l'organisation les met en place (voir §4.2.2 page126) et sont demandeurs d'informations et de sensibilisation. Il est indispensable de mettre en place des campagnes de sensibilisation, dès l'entrée des acteurs dans l'organisation et tout au long de leur vie dans

l'entreprise. Les menaces évoluent, donc la sensibilisation doit s'adapter.

Des budgets conséquents ne sont pas indispensables, pour mener lancer une campagne. L'imagination, la connaissance du terrain et des outils existants peuvent être un bon début (page §3.5 page 111, Annexe n°14 page 189).

CHAPITRE 5
EXPERIMENTER LA SENSIBILISATION

« Il y a ceux qui voient les choses telles qu'elles sont et se demandent pourquoi, il y a ceux qui imaginent les choses telles qu'elles pourraient être et se disent… Pourquoi pas ? »
Bernard Shaw[243]

[243] George Bernard Shaw (1856 -1950) est un critique musical, dramaturge, essayiste, auteur de pièces de théâtre et scénariste irlandais. Acerbe et provocateur, pacifiste et anticonformiste, il obtient le prix Nobel de littérature en 1925.

5.1. INTRODUCTION

Nous avons expérimenté la sensibilisation de la protection de l'information en se basant sur les recommandations des méthodes citées plus haut : Andragogie, ADKAR, Genba walk, Design Thinking en tenant compte de l'équation du changement (voir CHAPITRE 3 page 80) et nous nous sommes posés comme spectateur d'une approche menée par le Cabinet Carmignac afin de comparer le résultat des deux approches.

L'expérimentation a été effectuée par bribes, suite au changement d'emploi à deux reprises depuis 2017. Les retours d'expérience des acteurs qui ont participé à la construction des campagnes, ou à leur conception ou à la validation d'idées seront exposés dans les paragraphes suivants.

5.2. CONTEXTE

Neuf établissements de santé et une société privée, sont concernés par les parcours du patient traceur :

- Le GHT Saône-et-Loire Bresse Morvan s'étend du CH d'Autun à celui de Louhans avec parmi ses membres les CH de Chalon-sur-Saône et Montceau-les-Mines, Toulon-sur-Arroux, La Guiche, Chagny et le CHS de Sevrey. Le GHT représente 5 300 personnes environ.

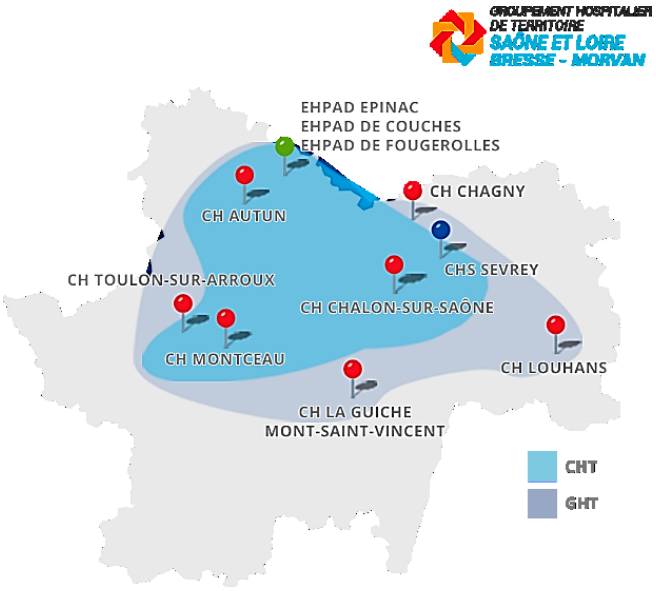


Figure 3 Groupement hospitalier de territoire de Saône et Loire Bresse - Morvan

- L'hôpital Européen de Marseille est un centre hospitalier privé à but non lucratif, constitué de plus de 1 000 salariés et 300 médecins libéraux.
- Et l'entreprise Carmignac est une entreprise privée (voir : L'organisation accompagnée : Société Carmignac, gestionnaire d'actifs page 77).

5.3. DEMARCHE

Comme l'indiquent les méthodes décrites au CHAPITRE 3, nous devons connaître nos interlocuteurs, leur environnement et relever des exemples dans lesquels nos acteurs pourront se projeter avant de construire le contenu de la campagne de sensibilisation adapté à notre cible.

Par ailleurs, nous devons identifier les ressources sur lesquelles nous pourrons nous appuyer, ou pas, ainsi que les moyens financiers alloués à la protection de l'information.

Les informations concernant, la maturité des sites, la cartographie applicative et les flux applicatifs

internes et externes peuvent être obtenues auprès de la personne responsable de la sécurité ou du directeur du système d'information de l'organisation. Ces informations étaient inexistantes ou incomplètes, c'est pourquoi le début de la démarche a été de compléter nos informations.

➔ *ANALYSE PREALABLE*

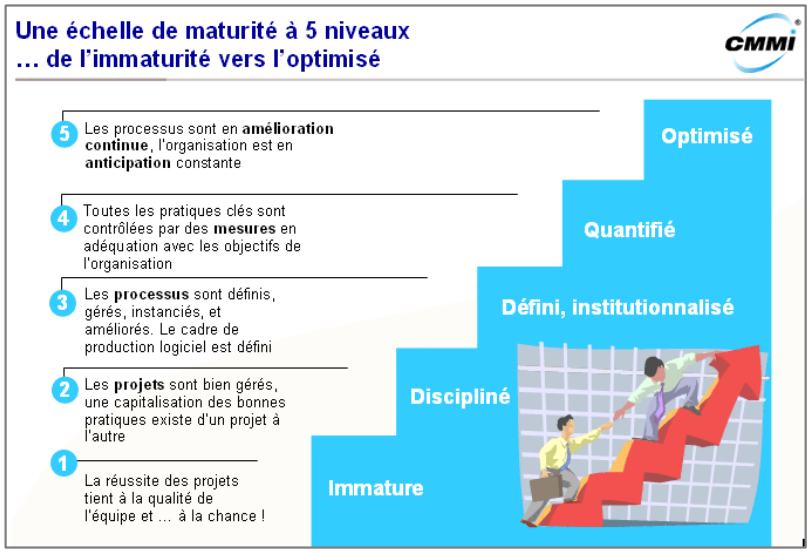
- **Niveau de maturité de ces sites (CMMI)**

Nous avons effectué un état des lieux de chaque établissement, afin d'appréhender, le niveau de maturité de ces sites (CMMI).

Le résultat de l'étude de la maturité des sites, effectuée par Monsieur Benjamin Malot, Responsable du Système d'Information du Groupement Hospitalier de Territoire (GHT) Nord Morvan, a été utilisé dans le cadre de la connaissance du système d'information des sites observés.

Monsieur Malot a analysé les moyens existants et la maturité de chaque système d'information dans le cadre de la mise en place de la Communauté Hospitalière de Territoire (CHT) en mai juin 2015. L'évolution de cette maturité ayant peu évolué au moment de l'écriture de ce document, nous avons utilisé ces informations.

La comparaison de la maturité du système d'information avec les bonnes pratiques nationales / internationales s'est faite par rapport au modèle CMMI[244] (Capability Maturity Model Integration). D'après la définition donnée dans le CMMI, « *la maturité d'une organisation est le degré auquel celle-ci a déployé explicitement et de façon cohérente, des processus qui sont documentés, gérés, mesurés, contrôlés et continuellement améliorés* ».



ID n° 81 : Schéma représentant les 5 niveaux de maturité du modèle CMMI

Ce référentiel définit la maturité du Système d'Information sur 5 niveaux.

L'audit est basé sur une analyse organisationnelle et technique.

Une note a été affectée sur l'aspect des procédures, la couverture des outils et l'organisation, ce qui a permis de définir la maturité du processus. La considération de l'ensemble des notes a permis d'évaluer la maturité de chaque site, et ainsi les comparer sur une base commune. Le résultat est

244 Cours à la Sorbonne UE5 GOUVERNANCE DES SIC par Alain Chetcuti

proportionnel au résultat numérique de la fiche d'interview.

À ce jour, le système d'information des sites de Montceau et Autun est situé entre 1 et 2, et celui de Chalon serait plus proche de 3.

Le manque de temps ne nous a pas permis de mener la même démarche auprès de l'hôpital Européen de Marseille. Au vu des premières observations et du résultat de l'audit technique et organisationnel mené en juin 2018, le niveau peut être estimé à 1. Cet établissement de santé a souscrit une assurance Cyber sécurité à la différence des établissements du secteur publique.

L'analyse du management de la protection de l'information des sites révèle une grande disparité de maturité.

Un séminaire d'accueil est organisé tous les six mois au mieux (Chalon sur Saône) ou pas du tout pour les autres sites, dans lesquels aucune sensibilisation à la protection de l'information n'est effectuée.

- **Protection de l'information dans le contexte de la norme ISO 27002**

Nous avons mené un audit flash, basé sur le SMSI ISO 27002 sur l'ensemble des sites entre octobre 2016 et avril 2018, pour compléter la vision en matière de sécurisation du système d'information et de la protection de l'information pour chaque site.

Les résultats vont de à 1,12 à 2,12 pour le plus haut, sur une cible moyenne proposée de 2,68.

- **Cartographie applicative**

Nous avons dressé une cartographie applicative, afin de visualiser l'écosystème des établissements, les outils utilisés par les acteurs et où sont les informations sensibles à protéger. Ces indications permettront de relever des exemples utilisés dans la campagne (andragogie).

- **Flux applicatifs interne et externe**

Nous avons inventorié les flux applicatifs interne et externe, afin de comprendre qu'elles sont les interactions, les flux critiques afin que les acteurs appréhendent la conséquence de leur acte sur les informations qui transite. Le Design Thinking est utilisé pour visualiser simplement ces flux.

- **Ressources humaines**

Nous avons étudié les moyens humains (ressources dans l'équation du changement) sur lesquels nous pourrons nous reposer ou utiliser comme relais dans les campagnes de sensibilisation en s'inspirant de l'organisation mise en place par la SNCF (voir

Mise en place d'un réseau de relais dans les services page 107). Nous pourrons nous appuyer sur les animateurs des parcours du patient traceur lorsque ceux-ci sont désignés et en cours (voir §5.4.2 page 154).

  - GHT

    Un RSSI est nommé dans ce cadre du GHT et gère l'ensemble des sites (9 établissements, 3 500 personnes environ) ainsi qu'un DPO (Data Protection Officer). Les cadres locaux ou le Directeur, pour les petites structures font office de relais. Donc leur temps est compté, ce point est à prendre en compte dans la campagne.

  - Hôpital européen

    Le RSSI est le responsable réseau. Il n'est pas la personne adéquate au vu des compétences

requises que nous avons décrites au paragraphe « étape 0 : quel profil pour sensibiliser les acteurs de l'entreprise ? » page 104.

Le RSSI consacre à peine 5 % de son temps au poste de protecteur de l'information et n'a jamais organisé de campagne de sensibilisation. Un DPO a été nommé au sein de l'établissement.

La structure n'organise pas de séminaire d'accueil pour les nouveaux arrivants ni de campagne.

- **Les moyens financiers**

Il est difficile d'obtenir des informations précises, au vu de la méconnaissance des organisations à identifier les coûts liés à la sécurité de la protection de l'information et du niveau de maturité des sites en matière de protection de l'information. Ce point rejoint le constat effectué par le CLUSIF (voir §4.5 page 142) :

- GHT

  Un budget est prévu pour la protection technique (en hausse de 2 % et concentré à Chalon sur Saône) mais aucun pour une campagne de sensibilisation. Le protecteur de l'information, ici le RSSI de territoire doit faire preuve d'imagination et de débrouillardise pour utiliser les outils en place (messagerie, intranet, centre de reprographie et de communication lorsqu'ils existent), du matériel gratuit (voir Annexe n°14 page 189) et de sa volonté à aller au-devant des utilisateurs sur les sites.

- Hôpital européen

  Ici aussi aucune campagne de sensibilisation n'a été effectuée. L'approche financière dans cet établissement diffère du secteur public ; l'hôpital fait souvent appel à des commanditaires et le service communication peut négocier un budget à consacrer à certaines actions de sensibilisation. Un budget est également consacré à la protection technique en augmentation de 0,87 % entre 2016 et 2017, et de 0,84 % entre 2017 et 2018.

➔ *LES PARCOURS*

Plusieurs avantages sont visibles dans l'approche de sensibilisation via des parcours et sont en adéquation avec les méthodes étudiées au CHAPITRE 3 page 80 :

Le responsable de la protection de l'information :

ACTIONS	METHODES
Est sur le terrain « là où se trouve la réalité » voir le processus réel	Genba Walk
Appréhende le travail des acteurs, leur personnalité, leurs difficultés, pose des questions et d'apprendre sur place.	Genba Walk
Chaque individu est considéré pour ce qu'il est, avec son potentiel d'apprentissage.	PEI (Programme d'Enrichissement Instrumental)
Tisse des liens de confiance avec ces personnes et peut relever des exemples d'actions à risques dans leur contexte.	Andragogie
Est transparent et bienveillant envers les équipes impliquées.	Andragogie
Favorise une adhésion à la méthode des personnes concernées.	ADKAR, Equation du changement, Design Thinking.

ACTIONS	METHODES
- Les résultats de l'analyse sont comparés aux bonnes pratiques et permettent d'inscrire la démarche dans un programme d'amélioration de la qualité.	- Référence à la roue de Deming245).

PARCOURS « PATIENT TRACEUR »

Cette méthode est apparue avec la mise en place de la certification des établissements de santé et s'appuie sur la *Joint Commission aux Etats-Unis* (Joint Commission 2008[246]). Elle permet de suivre un patient de l'amont de son hospitalisation jusqu'à sa sortie et d'analyser l'ensemble des actions entreprises durant ce parcours. Elle prend en compte l'expérience du patient et permet de réunir l'équipe de professionnels autour de la prise en charge du patient.

- Le responsable de la protection de l'information, est sur le terrain auprès des équipes. Il peut s'inspirer de cette méthode ou profiter d'un parcours de patient traceur pour s'immiscer dans le parcours en ajoutant un thème supplémentaire sur la protection de l'information.

a) Démarche de la méthode

Dans un premier temps, l'expert rencontre le patient volontaire, à qui il explique la méthode et sa finalité. La rencontre avec l'équipe impliquée dans le parcours et le patient favorise un vrai échange, voir un partenariat.

- Le responsable de la protection de l'information, peut intervenir auprès du patient et lui expliquer sa démarche. Une réunion préalable avec l'équipe est nécessaire pour expliquer les objectifs de l'interview du patient.
- Le patient peut être un gardien de l'information également, s'il est informé des dangers éventuels de l'utilisation de ses informations personnelles.

Les entretiens avec le patient sont utilisés dans l'analyse finale et le compte rendu avec l'équipe de la prise en charge du patient.

- Le responsable de la protection de l'information prépare des questions pour le patient.
- Exemple : Qu'avez-vous fourni comme type de document à l'hôpital ? Savez-vous où sont enregistrées vos informations personnelles ? Vous a-t-on informé de l'usage de vos documents ou données personnelles ? Avez-vous accès à vos informations de chez vous ?
- Les exemples recueillis seront utilisés en réunion. Parfois les acteurs de l'hôpital n'ont pas conscience de leur acte (exemple : documents de santé ou contenant des informations confidentielles laissées à la vue de tous au bureau d'accueil, sur la photocopieuse…).

L'analyse est en fait une discussion entre l'expert et l'équipe. Les points positifs, et à améliorer, sont mis en exergue afin d'initier, ensemble, un plan d'action.

Des animateurs externes à la prise en charge du patient peuvent être impliqués dans la démarche.

---

245 La roue de Deming (de l'anglais Deming wheel) est une transposition graphique de la méthode de gestion de la qualité dite PDCA (plan-do-check-act). Le cycle PDCA sert à transformer une idée en action et l'action en connaissance. Source Wikipédia

246 La « Joint Commission » est un organisme sans but lucratif basé aux États-Unis. La majorité des états américains demandent aux organismes de santé leur accréditation comme condition pour exercer et le remboursement des frais de santé. https://www.jointcommission.org/.

Cette organisation nécessite une forte implication des équipes, et du temps pour travailler ensemble (2 heures à 2 heures 30 de réunion).[247].

b) Après le patient traceur

Un plan d'action est finalisé, et des pilotes, pour mettre en œuvre ce plan et le suivre sont désignés. Après quoi, un retour est effectué, à l'ensemble de l'équipe impliquée dans la prise en charge du patient. Le service qualité vient en support méthodologique auprès des pilotes.

Une fiche de restitution du parcours est rédigée collégialement avec un plan d'action à suivre (voir Annexe n°24 page 212).

- La fiche de restitution comportera les dysfonctionnements relevés concernant la protection de l'information avec le plan d'action et les pilotes.
- L'ensemble des comportements à risques de tous les parcours seront collectés pour les campagnes de sensibilisation à grande échelle, sans nommer les équipes ou personnes à l'origine de ceux-ci.

c) Animateur de la réunion d'équipe

Un animateur (ou un binôme), reconnu par ses pairs est désigné pour coordonner le parcours, et faciliter la fluidité des échanges entre les professionnels. Cette personne ou binôme doit être formée à la méthode et en capacité à animer un groupe et favoriser un climat de confiance favorisant les échanges constructifs.

Les rôles sont distribués, s'il s'agit d'un binôme : un prend des notes et l'autre anime. Le binôme est constitué d'une personne externe à la prise en charge du patient et un soignant qui ne fait pas partie de l'équipe auditée. Cela permet de prendre du recul vis-à-vis des évènements remontés et favorise l'impartialité.

- Le responsable de la protection de l'information pourra s'appuyer sur ce binôme pour diffuser les messages durant les réunions post-parcours. Plusieurs réunions préalables seront nécessaires pour les former à protection de l'information et aux objectifs à atteindre.

d) Satisfaction des professionnels vis-à-vis de la méthode du patient traceur

La majorité des professionnels sont satisfaits de cette méthode, car ils la trouvent concrète et motivante. Des actions immédiates sont relevées, par rapport à des bonnes pratiques et cela permet d'améliorer le parcours de soins des patients.[248]

De plus, cette méthode donne la possibilité de visualiser un parcours dans sa globalité et non plus, de manière parcellaire à chaque état du patient dans son parcours.

Au point de vue du service, la cohésion de l'équipe est accentuée et chaque individu est mis en relief et se sent reconnu et impliqué dans le parcours comme un maillon de la chaîne.

---

247 Un exemple de grille est visible sur https://www.has-sante.fr/portail/plugins/ModuleXitiKLEE/types/FileDocument/doXiti.jsp?id=c_2794944. Une vidéo explicative : https://vimeo.com/88270918

248 Voir bilan complet de la satisfaction des acteurs du patient traceur à la fin de l'expérimentation : https://www.has-sante.fr/portail/upload/docs/application/pdf/2015-01/rapport_experimentation_methode_patient_traceur.pdf

La restitution est effectuée sous la forme d'une fiche pratique.

- Les professionnels sont impliqués directement dans leur pratique.
- La sensibilisation et la mise en lumière immédiate des actions à risques sont effectuées dans un processus de remise en question vis-à-vis des bonnes pratiques reconnues. Le message passe mieux car les réunions seront dans la bienveillance et l'unique objectif de s'améliorer.

Deux types de parcours, courants, ont été pris en compte dans l'approche de cette méthode, les consultations externes et l'admission des patients par le service des urgences :

Une consultation externe peut se terminer de deux manières : la sortie du patient de l'établissement ou une décision d'hospitalisation.

La prise en charge d'un patient par le service des urgences est très proche d'une consultation externe : du point de vue du système d'information, seule la procédure d'admission sera légèrement différente.

Nous n'envisageons pas un décès dans le cadre du patient traceur, donc la sortie sera toujours vers le domicile ou un autre établissement. Le patient choisi est toujours un patient ayant un parcours complexe et proche de la sortie de l'établissement.

L'admission aux urgences suit généralement une procédure simplifiée. Dans les cas de réelle urgence, certains établissements procèdent à une identification sommaire du patient, afin d'ouvrir un dossier médical informatisé et apporter immédiatement les soins nécessaires au patient. Lorsque cela devient possible, on procède à l'admission administrative.

PARCOURS « MOUVEMENT DE PERSONNELS »

La méthode du parcours peut être extrapolée à tout type de parcours comme la facturation, le mouvement des personnels, la visite d'un client, la visite d'une usine, l'organisation d'un évènement… Ici, elle a été appliquée aux personnels supports sur le parcours de mouvement de personnels « flux personnel non médical » de la même façon que le patient traceur.

La difficulté a été d'identifier les personnes en charge des différents parcours, car à chaque type de parcours des personnes différentes de secteur différents de l'organisation sont mobilisées.

Le parcours « flux personnel non médical » concerne deux personnes du service des ressources humaines.

Nous avons choisi le parcours de mouvement de personnel car c'est un sujet générique[249] dans toutes les organisations et un risque remonté dans le cadre du patient traceur.

La démarche identique au patient traceur a été menée auprès des personnels support du service des ressources humaines. Chaque type de mouvement de personnels a été analysé, ensemble, et les observations ou dysfonctionnement ont permis de sensibiliser les acteurs. Les faits ont été utilisés pour cette démarche de sensibilisation.

---

[249] Le CLUSIF définit la gestion des identités comme la gestion du « cycle de vie des personnes (embauche, promotion, mutation, départ, etc.) au sein de l'organisation et les impacts induits sur le système d'information ». Ces changements ont des conséquences sur les informations connues et gérées par le domaine d'identité de l'organisation. Source Gestion des identités. A. Balat, R. Bergeron, A. Butel, M. Cottreau, F. Depierre, G. Khouberman, L. Mourer, W. Poloczanski. CLUSIF, 63 pages, 2007

5.4. CAMPAGNE DE SENSIBILISATION

5.4.1. PREAMBULE

➔ *GHT GROUPEMENT HOSPITALIER DE TERRITOIRE*

Cette campagne est adaptée à notre cible, au contexte et répondant aux objectifs de protection de l'information. La démarche de préparation de la campagne ne s'est pas déroulée pendant le parcours du patient traceur, car la certification a été menée après le départ du RSSI.

« L'esprit de cette démarche » a été utilisé en amont, en interaction avec les Directeurs, Cadres de santé et Responsables informatique des sites, sur le cycle des parcours choisis pour la certification.

Le retour d'expérience est parcellaire, faute du temps nécessaire, la préparation de la mise en œuvre du RGPD et du départ du RSSI du GHT en avril 2018.

Aucun budget n'était prévu en 2016 et 2017 pour mettre en place une campagne de sensibilisation, donc les propositions sont basées sur le temps alloué au RSSI et l'imagination et la débrouillardise de celui-ci. La campagne commune, elle, est une vue à plus long terme et expose des propositions avec des outils payants supplémentaires (formation en ligne).

➔ *HOPITAL EUROPEEN*

Le service de communication, le DPO, le RSSI et le DSI de l'établissement ont bâti une campagne de sensibilisation entre avril et septembre 2018 pour une diffusion en janvier 2019. Cette campagne a été nommée « *le mois blanc* ».

Nous nous sommes inspirés du principe des campagnes menées par l'ANSSI annuellement. Ce mois de sensibilisation sera organisé en 4 temps : 1 thème abordé par semaine. Pour clôturer cet événement, une journée d'information sera organisée dans le hall à destination du grand public, du personnel et des médecins de l'hôpital.

Les retours d'expérience sont parcellaires ; nous avons décidé, toutefois de vous exposer ce projet de campagne car celui-ci correspond à une autre vision de la sensibilisation des acteurs de l'organisation tout en respectant les méthodes évoquées au CHAPITRE 3 page 80. Certaines idées sont issues des interviews, sondages et retours d'expériences des professionnels de la sécurité ou des acteurs de l'organisation (§2.4 page 63).

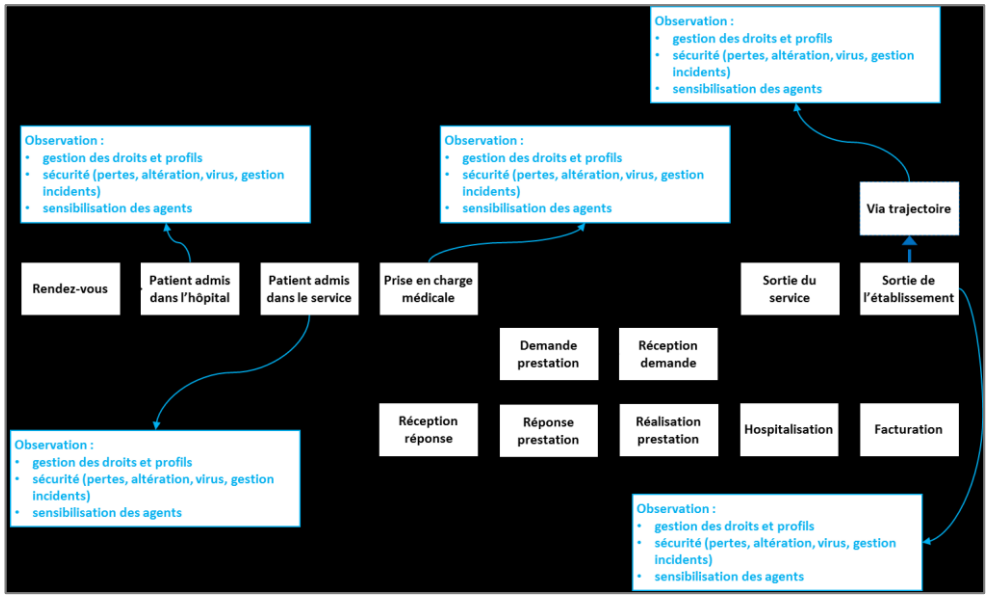
5.4.2. SENSIBILISATION PAR LES PARCOURS

Nous avons identifié avec la Direction Qualité de l'hôpital de Chalon sur Saône deux parcours patients traceurs pour expérimenter la sensibilisation. Ces parcours peuvent être expérimentés sur l'ensemble des sites du GHT.

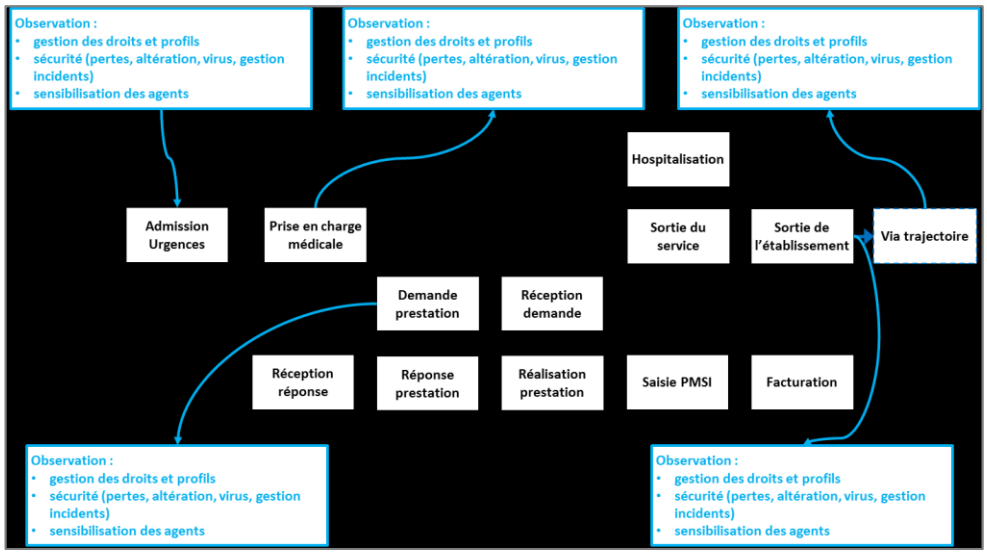
Cette approche a également été validée, dans un second temps, par le DPO de l'hôpital Européen de Marseille, dans le cadre de la préparation de la campagne de sensibilisation. L'action de sensibilisation est commune au responsable de la protection de l'information et au DPO dans le cadre de la mise en place du RGPD.

Sur le même principe du patient traceur, nous avons identifié un parcours « support » transposable à toute organisation : le parcours « mouvement de personnels » dans une organisation.

➔ *PARCOURS « PATIENT TRACEUR »*



ID n° 82 Parcours du patient traceur en consultation externe suivi d'une hospitalisation (source Chalon sur Saône).



ID n° 83 Prise en charge aux urgences (source Chalon sur Saône) [250]

Les carrés bleus sont les points d'observation à relever durant un parcours d'hospitalisation. L'observation peut être visuelle ou découler d'une question, par exemple :

- Comment la personne se connecte sur une application ?
- Quelle est votre profession et rôle dans le parcours ?
- Qui vous a donné les droits d'accès dans l'application ?
- Que faites-vous dans l'application ?
- Quels documents collectez-vous, où les stockez-vous et sous quel format ?

Les informations collectées ont été utilisées pour la certification.

---

250 • Via trajectoire (parcours programme) : ce parcours permet d'identifier facilement le ou les établissements capables de prendre en charge le projet de rééducation, réadaptation, réinsertion ou d'hébergement, nécessaire à différents moments de la vie de chaque personne.

L'ensemble des observations effectuées sur le parcours a été collecté dans un tableau Excel (voir Annexe n°16 page 194). Les actions immédiatement corrigeables seront vues en réunion post-parcours patient traceur et notifiées sur la fiche de restitution ; les autres dysfonctionnements ont fait l'objet d'un plan d'action à plus long terme.

Afin de sécuriser l'origine des données, les établissements n'ont pas été nommés, leur nom est remplacé par une lettre.

Trois grands thèmes à risque sont apparus durant l'ensemble des parcours et peuvent être exploités dans la campagne de sensibilisation :

1 - LA GESTION DES DROITS ET PROFILS : GERER L'ACCES A L'INFORMATION.

Les soignants utilisent l'identifiant et le mot de passe de leur collègue (en cas de remplacement ou d'absence), des comptes sont actifs sans utilisateurs ou ont un excès de droits non justifiés par le métier.

a) Actions de sensibilisation :

Nous pouvons nous appuyer sur les actions ci-après, pour sensibiliser les médecins et les autres soignants sur cette pratique en mettant en exergue leur responsabilité :

- Tester la modification d'une prescription médicale sur un dossier patient test et visualiser du nom qui apparaît sur les documents et les données de connexion,
- Soumettre les participants aux scénarios d'incidents que nous avions utilisés dans la mesure de la sensibilisation, notamment celui concernant l'« usurpation d'identité » et les « stagiaires et intérimaires » (voir §4.2.2 page 126)
- Diffuser des supports de communication courts (2 à 3 minutes maximum) pendant la restitution (voir Annexe n°14 page 189[251]) sur la gestion des mots de passe et les données patients[252], et sur la *« Sensibilisation Sécurité information : Piratage informatique, protégez votre entreprise »* [253]
- Positionner l'affiche « *Accepteriez-vous de prêter votre brosse à dents ? Les mots de passe et les brosses à dents ont beaucoup de points communs ! Il faut les choisir avec soin et les changer régulièrement, ne pas les partager et surtout… Les utiliser* »[254] dans le bureau du cadre,
- Transposer la problématique dans leur vie privée[255] (identifiant avec un mot de passe unique, vols sur les comptes bancaires, ordinateur familial…). Nous pouvons nous appuyer sur les usages identifiés lors du sondage (voir §4.2.1 page 123).

b) Retours attendus :

- Prise de conscience des acteurs sur l'usage de leur identifiant personnel par une tierce personne qui pourrait engager leur responsabilité.

---

251 Exemple : Attitude 3d - Le programme SNCF de sensibilisation à la protection de l'information https://youtu.be/egW8fTtYrac et Vidéo de démonstration de Conscio Technologies https://youtu.be/odLNqtM8wZk

252 Vidéo à regarder https://youtu.be/GubySVnMypg

253 Vidéo de la société Conscio Technologies https://youtu.be/Zn8OSTB6ekg (arrêté après 2 :13 minutes)

254 Voir affiche http://www.esante-bourgogne.fr//wp-content/uploads/2016/03/GCS-SSI-Affiche-sensibilisation-mots-de-passe-v1.jpg

255 Explication de la fiche CNIL sur les mots de passe : https://www.cnil.fr/fr/pourquoi-securiser-au-maximum-le-mot-de-passe-de-votre-boite-courriel

- Prise de conscience de la nécessité de sécuriser leur sphère privée qui est soumise, aussi, à l'usage d'identifiant et de mot de passe (gestion de comptes bancaires, messagerie personnelle…).

c) Actions proposées :

- Actions de sensibilisation (ci-dessus)
- Un coffre-fort électronique pour gérer les mots de passe (Keepass, Dashlane professionnel…),
- Outils de centralisation des habilitations prévues dans le cadre de l'harmonisation des logiciels dans le GHT (Groupement Hospitalier de Territoire).

d) Retours sur les actions proposées

- Le Directeur et la Directrice qualité de l'EHPAD de la Guiche Mont Saint Vincent, Le Directeur qualité de l'hôpital de Montceau les mines, ainsi que certains médecins (oncologues et urgentistes) nous ont fait part de la satisfaction des propositions avancées.
- Ces personnes utilisent des applications sensibles et sont motrices dans les établissements. Ces personnes se feront le relais des campagnes de sensibilisation sur la gestion des accès aux applications.

2 - LA DEGRADATION DE L'INFORMATION ET GESTION : PERTE OU ALTERATION D'INFORMATION, CONTAMINATION PAR DES VIRUS ET GESTION D'INCIDENTS EN CAS D'INCIDENT MAJEUR,

Les soignants ne verrouillent pas leur ordinateur lorsqu'ils se rendent au pied du patient et laisse le matériel à la vue de tous dans le couloir. L'accès au système d'information et la visualisation de données confidentielles sont possibles. La messagerie du soignant est parfois ouverte sur l'appareil également.

a) Actions de sensibilisation :

Nous pouvons nous appuyer sur les actions ci-après, pour sensibiliser les médecins et les autres soignants sur cette pratique :

- Profiter de l'absence du soignant devant la machine pour utiliser sa messagerie et envoyer des messages amicaux à d'autres acteurs de l'établissement (invitation à boire un café au service restauration de l'hôpital). La sensibilisation se fera à la restitution lorsque la personne nous fera part des retours de ses collègues contactés par nos soins. Le message aurait pu être envoyé à des personnes extérieures avec des données de l'hôpital ou des menaces, injures…
- Changer le fond d'écran de l'ordinateur par une image sur le verrouillage de session [256] dont le thème est « *Quitteriez-vous votre maison sans fermer la porte à clef ? Nos comptes informatiques donnent accès à des données sensibles. Il faut donc protéger son ordinateur professionnel comme sa maison : verrouillons nos sessions* ». Une affiche a été positionnée dans les salles de pause [257] « *Laisseriez-vous le public assister à votre opération ? Les patients nous font confiance protégeons leurs données de santé. Les info*rmations relatives à l'état de santé physique et psychique d'un

[256] Affiche visible sur : http://www.esante-bourgogne.fr//wp-content/uploads/2016/03/GCS-SSI-Affiche-sensibilisation-verrouillage-de-session-v1.jpg

[257] Affiche visible sur : http://www.esante-bourgogne.fr//wp-content/uploads/2016/03/GCS-SSI-Affiche-sensibilisation-donn%C3%A9es-de-sant%C3%A9-v1.jpg

patient sont considérées comme des informations sensibles. Nous devons en assurer la confidentialité conformément au code de la santé public et de la CNIL ».

- Visualiser la vidéo sur les consignes de base [258]

b) Retours attendus :

- La modification de l'image en fond d'écran devrait alerter les soignants que l'ordinateur a été manipulé par une tierce personne en leur absence. Cette action devrait sensibiliser les personnes sur la nécessité de sécuriser leur outil informatique en cas d'absence de leur part.

c) Actions proposées :

- Revoir le temps de la mise en marche de l'écran de veille avec un mot de passe des ordinateurs portables.
- Un plan à plus long terme a été mis en place sur la gestion de l'accès à l'ordinateur grâce à une carte (carte CPS), afin de faciliter l'usage des outils informatiques pour les soignants tout en protégeant l'information.

d) Retours sur les actions proposées :

- Le Directeur qualité de l'hôpital de Montceau les mines, ainsi que le président de CME nous ont fait part de la satisfaction des propositions avancées.
- Les médecins sont demandeurs d'outils facilitant la protection de l'information, donc ils seront moteurs sur le sujet.

3 - LE MANQUE DE SENSIBILISATION DES AGENTS A LA PROTECTION DE L'INFORMATION.

- Une première de campagne de sensibilisation sera proposée sur les grands thèmes à risque apparus durant les parcours ci-dessus, basé sur les scénarios d'incident (voir §4.2.2 page 126) et sur les réponses apportées par les internautes (voir §4.2.1 page 123),
- L'ensemble des observations et réponses ont été collectées durant les parcours et consignées dans un tableau Excel afin de servir de base de travail,
- Une enquête a été menée auprès des différents acteurs des établissements, afin de connaître les actions existantes ou moyens de protection mis en place,
- Un plan d'action pour chaque risque a été mis en place, comportant des indicateurs à vérifier périodiquement afin de mesurer l'atteinte des objectifs,
- La campagne de sensibilisation à l'ensemble des sites du GHT sera menée conjointement avec le DPO car les points relevés sont communs aux deux protecteurs de l'information (§5.4.3 page 162).

➔ *PARCOURS « MOUVEMENT DE PERSONNELS » DE MONTCEAU LES MINES*

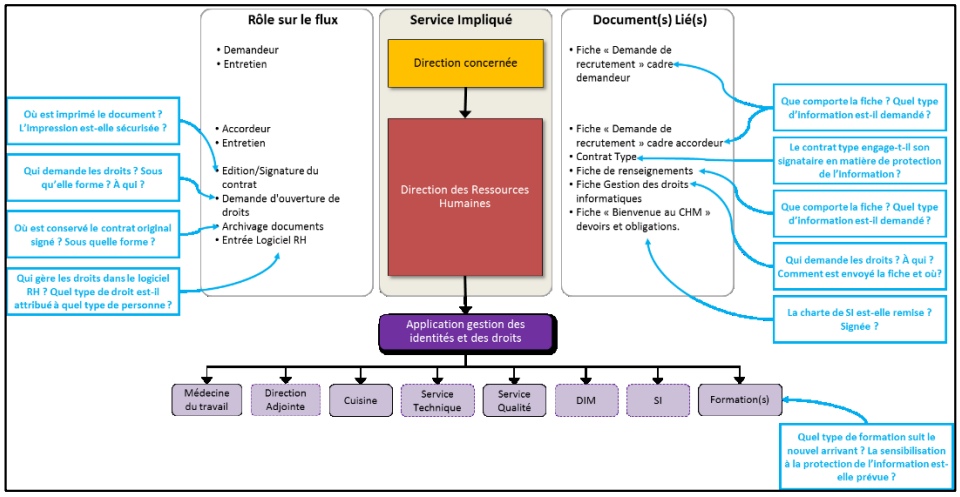
Ce parcours a été identifié dans le cadre d'un projet de gestion des mouvements des personnels de l'hôpital de Montceau en 2014. Ce projet était toujours identique et à l'arrêt en octobre 2016 par manque de budget et de ressources nécessaires à son déroulement.

L'identification des problématiques de protection de l'information a été effectuée, malgré tout, auprès des deux responsables du service des ressources humaines. L'étude a été menée dans leur bureau en septembre 2014 afin de visualiser leur environnement de travail et identifier les risques

[258] Vidéo de la société Conscio Technologies https://youtu.be/9r4KwAB5Yxl. Extrait gratuit sur le réseau YouTube d'une durée d'une minute.

éventuels pour la protection de l'information. L'analyse a été effectuée en 2017 dans le cadre de ce mémoire.

De ces constats une liste d'actions a été dressée dans le cadre de la construction d'une campagne de sensibilisation dirigée vers les personnels support, pour les points communs et vers les personnels RH pour les points métiers.



ID n° 84 analyse du flux des personnes médical

Les carrés bleus sont les points d'observation à relever durant un parcours. L'observation peut être visuelle ou découler d'une question, par exemple :

- Où est imprimé le document ? L'impression est-elle sécurisée ?
- Qui demande les droits ? Sous qu'elle forme ? À qui ?
- Où est conservé le contrat original signé ? Sous quelle forme ?
- Qui gère les droits dans le logiciel RH ? Quel type de droit est-il attribué à quel type de personne ?
- Que comporte la fiche ? Quel type d'information est-il demandé ?
- Qui demande les droits ? À qui ? Comment est envoyée la fiche et où ?
- La charte de SI est-elle remise ? Signée ?
- Quel type de formation suit le nouvel arrivant ? La sensibilisation à la protection de l'information est-elle prévue ?

Les réponses et observations ont été collectées dans un tableau Excel et une enquête a été menée auprès des différents acteurs des établissements, afin de connaître les actions possibles pour protéger les informations. Des indicateurs de mesure d'atteinte des objectifs ont été mis en place.

La campagne de sensibilisation de tout le personnel RH sera menée, ultérieurement, conjointement avec le DPO car les points relevés sont communs aux deux protecteurs de l'information.

Deux thèmes sortent du lot des observations. Les points recueillis sont globalement courants au vu des retours d'expériences vu précédemment (§2.4 page 63) dans les organisations :

1 - La gestion documentaire : L'impression securisee des documents, le stockage des documents (contrats de travail, arret maladie…) et la remise de document de sensibilisation, dont la charte informatique, aux nouveaux arrivants.

Le service des ressources humaines de l'hôpital de Montceau les mines est coincé entre des services de soins, ce qui est le cas également des autres services support.

Les personnes du service impriment sur une imprimante située dans le couloir à la vue du public de passage. Les imprimantes sont munies d'un système de déverrouillage par un mot de passe avant impression qui n'est pas utilisé par les acteurs du service des ressources humaines, car cette fonctionnalité est considérée comme mal pratique.

Les documents personnels des salariés sont stockés dans des armoires, non fermées à clefs dans les bureaux. Les locaux sont accessibles avec un pass par les personnels du service de ménage externalisé, du service de sécurité et du service informatique.

a) Actions de sensibilisation :

- Positionner un jeune stagiaire proche de l'imprimante avec la consigne, pendant une journée, de relever le délai ou les personnes viennent chercher leurs documents et ceux qui restent jusqu'au soir [259], au mieux, sur l'imprimante.
- Le stagiaire observera ce qu'il se passe vis-à-vis du public autour de l'imprimante. Nous avons pu observer, proche du service informatique, que certains visiteurs regardent les documents sur l'imprimante par curiosité ! Il faut dire que l'imprimante est positionnée juste avant les sanitaires !
- Tagger les documents non récupérés dans l'heure d'un post-it avec la mention « VUE ! Signé un mystérieux inconnu ! » et subtiliser les documents non récupérés en fin de journée.
- Accéder aux locaux en fin de journée avec un pass après le départ des personnels, modifié les fonds d'écrans des ordinateurs non verrouillés, positionnés des post-it sur des dossiers et les écrans d'ordinateurs avec la mention « VUE ! Signé un mystérieux inconnu ! ». Le service de sécurité sera prévenu de l'action en amont.
- La même action sera effectuée sur les documents dans les armoires, dont les portes sont laissées ouverte et non munie d'une serrure.
- Visionner la vidéo de la SNCF sur la « *Protection de l'information sensible* »[260] et sur les consignes de base de la société Conscio Technologies[261].

b) Retours attendus :

- Une réaction des acteurs le lendemain matin lors de leur prise de fonction à la vue des post-it et des armoires ouvertes.
- M. Kelles, RSSI de société Carmignac (§2.4.1 page 63) a mené un type d'action similaire :

---

259 En moyenne, on compte 12 000 pages imprimées par an et par employé 26% des salariés français déclarent avoir trouvé des documents confidentiels à la sortie des imprimantes. 38% des collaborateurs impriment tous leurs courriels et 25% des documents imprimés sont jetés dans les 5 minutes. Un salarié, en moyenne imprime 30 pages par jour et la gestion des documents représente un coût de 3 à 5% du chiffre d'affaire d'une organisation Source Gartner

260 SNCF https://youtu.be/0sWZ55molmw

261 Conscio Technologies https://youtu.be/9r4KwAB5YxI. Extrait gratuit sur le réseau YouTube d'une durée d'une minute

- Dans un premier temps des post-it ont été collés sur l'écran des ordinateurs non attachés par un câble de sécurité à la fermeture des bureaux, avec un rappel aux bonnes pratiques.
- Dans un deuxième temps, les ordinateurs non attachés ont été récupérés par le RSSI. Les propriétaires des machines sont venus récupérer leur ordinateur le lendemain matin et une sensibilisation à la protection des informations leur a été apportée.
- Monsieur Kelles, RSSI a constaté une diminution de ce phénomène au bout de quelques semaines.
- La société Wavestone conseille ce genre de procédé à ses clients.

c) Retours sur les actions proposées :

- Le principe de la sensibilisation a été validé par la Direction et accueilli avec satisfaction.
- La Direction n'avait pas conscience de cette faille (elle a une imprimante dans son bureau). La protection des informations des regards de curieux n'avait pas été envisagée.

2 - LA GESTION DES HABILITATIONS DU LOGICIEL DES RESSOURCES HUMAINES

Nous constatons que des comptes sont actifs sans utilisateurs ou ont un excès de droits non justifiés par le métier. L'usage de profil n'est pas utilisé, la gestion au logiciel est individualisée. Les personnes en charge de la gestion des accès au logiciel ne sont pas formées dans les règles de l'art sur ce module. Il n'y a pas d'obligation de modifier le mot de passe, identique pour tous les comptes, à la première connexion.

a) Actions de sensibilisation :

- S'introduire dans le bureau avec le pass, accéder au logiciel RH avec un compte fermé et modifier la fiche de deux nouveaux arrivés, dont la fiche est incomplète.

  La Direction sera informée de notre action au préalable.

  Le logiciel permet d'afficher les dernières fiches modifiées, ou ajoutées, sur un tableau de bord, afin de permettre à l'utilisateur de reprendre son activité là où il s'est arrêté avant de fermer le logiciel.

- Lors de la restitution, diffuser des supports de communication courts sur la protection des informations dans les logiciels (2 à 3 minutes maximum) (voir Annexe n°14 page 189[262]) sur :
  - La gestion des mots de passe[263].
  - La « Sensibilisation Sécurité information : Piratage informatique, protégez votre entreprise » de la société Conscio Technologies[264].
  - Proposer de jouer aux premiers scénarios du jeu de la CCI de Normandie sur Intelligence économique[265].
  - Soumettre les participants aux scénarios d'incidents que nous avions utilisés dans la mesure de la sensibilisation (voir §4.2.2 page 126) et débattre sur les résultats.

---

262 Exemple : Attitude 3d - Le programme SNCF de sensibilisation à la protection de l'information https://youtu.be/egW8fTtYrac et Vidéo de démonstration de Conscio Technologies https://youtu.be/odLNqtM8wZk

263 Vidéo à regarder https://youtu.be/GubySVnMypg

264 Conscio Technologies https://youtu.be/Zn8OSTB6ekg (arrêté après 2 :13 minutes)

265 CCI de Normandie http://www.jeu-ie.cci.fr/

b) Retours attendus :

- Découverte de la supercherie après un certain délai. Une non-réaction immédiate est courante car les cybers attaquants se montrent très discrets afin de s'infiltrer plus facilement et longuement dans le système d'information.
- Monsieur Cartau, RSSI et DPO du CHU de Nantes, (§2.4.1 page 63) a mené une action d'usurpation d'identité d'un Directeur d'établissement qui refusait de modifier son mot de passe (123456 !). M. Cartau s'est connecté sur un ordinateur à plusieurs reprises avec l'identifiant du Directeur et un mauvais mot de passe, afin de bloquer son compte. Le Directeur de l'établissement pensait qu'une personne malveillante essayait d'utiliser son compte et à changer son mot de passe de façon sécurisé.
- Les actions chocs sont parfois nécessaires pour arriver à ses fins !

c) Retours sur les actions proposées :

- Le principe de la sensibilisation a été validé par la Direction et bien accueilli. La Direction n'avait pas du tout conscience de cet aspect de gestion du logiciel RH et par extension d'autres applications métier.

5.4.3. CAMPAGNE COMMUNE DE SENSIBILISATION DES HOPITAUX DU GROUPEMENT HOSPITALIER DE TERRITOIRE DE SAONE ET LOIRE BRESSE - MORVAN

➔ *OBJECTIFS*

SENSIBILISER LES COLLABORATEURS :

- Présenter les enjeux et les risques auxquels les sites du GHT sont soumis,
- Convaincre de l'utilité des actions à tous les niveaux,
- Modifier les comportements et instaurer les bons réflexes en termes de protection de l'information,
- Responsabiliser l'ensemble des acteurs.

DEVELOPPER UNE « CULTURE DE PROTECTION DE L'INFORMATION » AU SEIN DES SITES DU GHT :

- Donner au Top Management une vision globale de la protection de l'information,
- Informer sur l'avancement et l'efficacité des initiatives en termes de protection de l'information,
- Orienter les décisions.

➔ *SYNTHESE DU PLAN DE SENSIBILISATION*

La proposition de campagne a été découpée en cinq types d'acteurs afin de cibler les métiers, le format de support de la sensibilisation, les coûts possibles et l'efficacité envisagée.

Les sujets relevés dans le cadre des parcours (§5.4.2 page 154) seront traités dans la campagne en priorité. Les sujets abordés seront par type de cible :

CIBLES	ACTIONS
Ensemble du personnel (tronc commun)	- Présentation des bonnes pratiques relatives à la protection de l'information - Messagerie électronique, gestion des mots de passe, internet, les périphériques et le poste de travail (les disques durs externes, les clés USB, etc.), Internet, les réseaux sociaux, l'ingénierie sociale266, - Comment protéger les informations en mobilité (réunion externe, voyage…), - Protections des données : rappels des aspects juridiques liés à l'utilisation du système d'information et rappels des règles à suivre (charte, PSSI, RGPD), - Sujets relevés dans le cadre des parcours.
Directeurs et Secrétariat de direction	- Etat de la menace - Rôles et responsabilités - Classification et protection des données sensibles - Présentation des règles à respecter en situation de mobilité - Continuité d'activité (PCA), comment protéger les informations en cas de sinistre, - + tronc commun
Populations métier sensibles : Achats, RH, Soins, Finances, Techniques, SI, Biomédicale	- Présentation des enjeux métiers spécifiques - Classification et protection des données sensibles - Réglementation (RGDP). - Finance : Mesures de réduction des risques de fraude au président - + tronc commun
DSI / sécurité du système d'information	- Usage raisonné et protection des accès privilégiés aux SI - Réglementation : RGDP, ARS, HAS - Dispositif de continuité d'activité - Processus de gestion de crise - Rôles et responsabilités en cas de PCA / crise. - + tronc commun

Les facteurs de succès suivants ont été identifiés suivant les retours d'expérience (voir §2.4 page 63) et les données remontées (voir §4.2 page 123) :

CIBLES	ACTIONS
Ensemble du personnel (tronc commun)	- Caractère obligatoire de la formation en ligne, - Outil de formation en ligne permettant de suivre les noms des personnes ayant suivi la formation et leurs résultats, - Relances automatiques des personnes n'ayant pas suivi la formation ou n'ayant pas obtenu des résultats suffisants, - Engagement de la direction (communication d'un membre de la direction en lancement de la campagne), - La durée de réalisation des modules de la formation en ligne ne devra pas excéder 15 à 20 minutes pour les participants.
Directeurs et Secrétariat de direction	- Présentations dans le cadre des comités sécurité, - Rôle de commanditaire du Top Management, - Mutualisation des présentations PCA et SSI.
Populations métier	- Identifier les populations concernées de manière exhaustive

[266] L'ingénierie sociale (ou social engineering en anglais), fait référence à des pratiques de manipulation psychologique à des fins d'escroquerie. Les pratiques d'ingénierie sociale exploitent les faiblesses psychologiques, sociales et plus largement organisationnelles pour permettre d'obtenir quelque chose de la personne ciblée (un bien, un service, un virement bancaire, un accès physique ou informatique, la divulgation d'informations confidentielles, etc.). En utilisant ses connaissances, son charisme, l'imposture et le culot, l'attaquant cherche à abuser de la confiance, de l'ignorance et de la crédulité des personnes possédant ce qu'il souhaite obtenir.1 source Wikipédia

CIBLES	ACTIONS
sensibles : Achats, RH, Soins, Finances, Techniques, SI, Biomédicale	- Andragogie : reprendre les points relevés lors de l'analyse des parcours - Messages formulés de façon synthétique - Mettre en évidence les principaux messages - Présentation attrayante réalisée en concertation avec l'équipe de communication (vidéo, prospectus, affiches…). - Mise à disposition de plaquettes à divers endroits (distribution sur les bureaux, mise à disposition sur l'intranet et dans les espaces communs, etc.) - Identifier les messages clés à adresser au service des finances qui peut être confronté aux risques de fraude au président. - La réalisation de tests à un fort impact sur les collaborateurs - Les sessions de présentation peuvent s'inscrire dans les réunions hebdomadaires animées par les responsables de départements ou être réalisées dans le cadre de réunions spécifiques.
DSI / sécurité du système d'information	- Les messages de sensibilisation sur le risque ingénierie sociale doivent également être relayés via les actions destinées à l'ensemble des collaborateurs. - La réalisation de tests à un fort impact sur les collaborateurs - Le PCA et les outils de gestion de crise devront être mis à jour après chaque exercice. - Les sessions de formations et de sensibilisation doivent être scindées en 2 à 3 sessions pour adresser l'ensemble des acteurs du PCA.

- **Outils utilisés pour la campagne :**

CIBLES	OUTILS UTILISES	FREQUENCE	EFFICACITE ATTENDUE
Ensemble du personnel	Formation en ligne (20 minutes en ~4 modules)	Annuelle	Moyenne à Forte
	Courriel, Impressions, Ecrans	À l'initialisation et pour les nouveaux arrivants Mensuelle	Faible à Moyenne
Directeurs & Secrétariat de direction	Présentiel	À l'initialisation Et Annuelle	Forte
Métiers sensibles : Achats, RH, Soins, Finances, Techniques, SI, Biomédicale	Plaquette	À l'initialisation et pour les nouveaux arrivants	Moyenne
	Courriel, Impressions, Capture d'écrans	Suivant l'actualité	Forte
	Bulletin d'information	Mensuel	Forte
DSI et sécurité du système d'information	Présentiel	Annuelle	Forte

➔ *SUPPORTS DE COMMUNICATION*

L'ensemble des supports de communication sera utilisé suivant leur efficacité attendue et les coûts engendrés. L'évaluation des coûts et efficacité indiquée par la société Wavestone sont retenues comme point d'évaluation budgétaire (voir le détail §4.3 page 133).

➔ *BUDGET PREVISIONNEL*

CHARGES ANNEE 1	CHARGES ANNEES SUIVANTES
77 jours homme + 10 000 € 350 heures pour les participants, soit un peu plus d'une heure en moyenne par participant	93,4 jours homme + 10 000 € 350 heures pour les participants, soit un peu plus d'une heure en moyenne par participant

Voir détail Annexe n°25 page 213.

➔ *RESSOURCES ET PILOTAGE*

Le pilotage sera réalisé par le RSSI :

- Lancement et suivi de l'avancement des actions de sensibilisation
- Suivi des KPI et évaluation des résultats (taux de participation à la formation en ligne, indicateurs comportementaux, etc.)
- Élaboration de plans d'actions en fonction des besoins exprimés (formation complémentaire, courriels de sensibilisation, etc.)

En proche collaboration avec les autres départements :

- Communication interne : assistance pour la formalisation des supports de sensibilisation (notamment graphistes).
- DSI : Rôle de pilote / communication des bonnes pratiques aux collaborateurs et remontée des besoins de formation complémentaires.
- RH : Communication de la charte informatique aux nouveaux arrivants et signature de cette charte et intégration du plan de sensibilisation SSI au plan de formation global IFSI et séminaire d'accueil.

➔ *ACTIONS PONCTUELLES DEJA LANCEES ER RETOUR D'EXPERIENCE*

Vu l'éloignement des sites, le courriel est le média le plus utilisé. Les messages sont lus et relayés en interne. Des actions ponctuelles ont été lancées en amont de la proposition de campagne.

- Edition d'un bulletin d'information sécurité et sensibilisation aux nouvelles technologies, dirigée vers la Direction des établissements et des responsables de service (voir Annexe n°26 page 213).
  - La Newsletter est appréciée du top management et des responsables de service, qui la font circuler dans l'établissement et même en dehors auprès de prestataires ou de leurs connaissances. Des nouvelles concernant la protection de l'information sont diffusées et également des informations sur des technologies moins usitées dans les établissements pour l'instant, comme l'IA, le machine learning, la Blockchain… afin de les sensibiliser par rapport à la protection de l'information qui va en découler.
- Envoi de courriels de sensibilisation « opportunistes », en cas d'identification d'un sujet ou d'un événement sur lequel communiquer (départ en vacances) a été adressé par courriel à l'ensemble des acteurs du GHT et diffusé auprès des relais locaux pour diffusion sur leur intranet,
  - Les Directeurs des petites structures du GHT apprécient d'être pris en compte et sont friands de ce type d'information.
  - Les messages sur l'intranet sont consultés, suivant les sujets d'actualité (mise en garde avant de partir en vacances, virus en cours, vigilance sur l'opération black Friday, etc.). Les utilisateurs adressent régulièrement des messages de remerciement au responsable de la protection de l'information ou des questions complémentaires. Ce média permet d'être présent régulièrement (l'intranet est la page d'accueil de l'explorateur Web).
- Sensibilisation sur les mots de passe,
- Diffusion de fiches pratiques, en cas d'incident auprès des responsables de services et des Responsables des systèmes d'information des sites,
  - Les fiches pratiques sont appréciées des relais sur les sites et des responsables du système d'information. Ils se sentent pris en considération et rassurés en cas d'incident. Un circuit

de remonté d'incident a été mis en place et des visites sur le terrain sont nécessaires pour établir une relation de confiance avec les acteurs locaux.

- Formalisation d'une charte informatique,
- Sensibilisation relative à la protection des données personnelles menée auprès des élèves de l'IFSI (école d'infirmières) par la personne en charge de la formation attachée à la DSI et en collaboration avec le protecteur de l'information.
  - La réaction des élèves de l'IFSI a été positive car ils n'imaginaient pas les pièges qui pouvaient être mis devant leur route et ils seront sensibilisés avant d'arriver à l'hôpital. Nous pourrons nous appuyer sur ces personnes pour diffuser des messages pour la protection des informations.
- Rencontre avec les Directeurs d'établissements, les cadres de santé et les Responsables des systèmes d'information dans le cadre de l'audit précertification HAS V2014. Ces rencontres ont permis de relever des dysfonctionnements pouvant mettre en danger les informations. Ces rencontres régulières ont permis de tisser des liens de confiance et de transmission des savoirs en matière de protection.

5.4.4. HOPITAL EUROPEEN DE MARSEILLE

➔ *OBJECTIFS*

L'objectif de la campagne est de :

- Sensibiliser de façon concrète le personnel, les médecins et les prestataires sur la protection des informations.
- Mettre en valeur les actions mises en place à l'Hôpital Européen.
- Présenter la nouvelle réglementation RGPD et les actions de l'Hôpital Européen pour répondre à ses nouvelles exigences.
- Le budget pour atteindre cet objectif n'est pas arrêté (coûts des éditions, personnel mobilisé, gadgets, comédiens et les t-shirts pour les organisateurs HE).

➔ *SYNTHESE DU PLAN DE SENSIBILISATION*

Il n'a pas été fait de distinguo entre les différents acteurs de l'organisation. Les patients seront aussi impliqués car, les animations se dérouleront essentiellement dans le hall de l'hôpital et ils seront acteurs dans le questionnement de la protection de leurs données à l'hôpital. Les représentants des usagers seront également sollicités, notamment dans le cadre de la protection des données personnelles.

Tout au long du mois, une boîte à idées sera mise à disposition pour le personnel avec pour thème « *Que pensez-vous faire pour la protection des données ?* ». Les meilleures idées seront affichées sur les stands lors de la journée d'information.

SEMAINE 1 THEME : PROTEGEZ VOTRE VIE PRIVEE ET CELLE DES AUTRES ! MOT DE PASSE, DISCRETION SUR LE WEB ET NOTAMMENT SUR LES RESEAUX SOCIAUX.

- **Actions :**
  - Intervention de la troupe de théâtre pour une petite représentation (hall ou cafétéria). Les scénarios choisis sont :
  - Scène dans le métro, un responsable de service reçoit un courriel confidentiel sur son ordiphone. Le message est également lu par d'autres personnes par-dessus l'épaule de la personne = discrétion dans les lieux publics.

- Scène dans le train ou deux médecins discutent d'un de leur patient connu. Les passagers derrière eux sont journalistes à sensation et entendent la conversation.
- Scène de réception d'un courriel frauduleux et les conséquences (voir partenariat avec Sophos)
- Créer un lieu avec différentes zones :
- Un lieu public avec un wifi ouvert non protégé et des actions de piratage
- Une zone d'échange sur les bonnes pratiques à adopter
- Attention aux wifi publics,
- Attention aux transferts de données de l'organisation par la messagerie non sécurisée, etc.

SEMAINE 2 THEME : LES SUPPORTS EXTERNES

- Clé USB, téléphones, ordinateurs portables, tablettes…
- Lien avec les restrictions de l'hôpital européen, les risques et comment s'en prévenir

- **Actions :**
  - Créer un « bureau des erreurs » dans lequel les participants devront identifier les dangers liés à la protection des informations.
  - Attaque via une clef USB simulant un cheval de Troie ou ransomware.

SEMAINE 3 THEME : NE TOUCHE PAS A MA MESSAGERIE !

- Les risques : pourriel, courriels frauduleux, virus
- Les protections : antivirus, vigilance face aux courriels frauduleux
- Idée pour une illustration : Courriel qui passe à la machine à laver

- **Actions :**
  - Marquer les esprits en organisant un « piratage » sur tous les postes de l'hôpital et/ou téléphones portables et/ou courriel malveillant « on vous a bien eu ! »

SEMAINE 4 JOURNEE D'INFORMATION ET THEME : OU SONT MES DONNEES ? CIRCULATION, CONSERVATION, ELIMINATION ET ARCHIVAGE DES INFORMATIONS

- **Actions :**
  - Démonstration d'ingénierie sociale sur le Directeur ou/et des personnes repérées et volontaires dans l'établissement (Facebook, internet, LinkedIn, GoogleMap) et jeu de rôle avec la troupe de théâtre.
  - Installation d'une zone d'information avec le service juridique de HE,
  - Hacking en direct par l'ANSSI de téléphone portable, de duplication de badge,
- Organisation d'un concours sous forme de questionnaire interactif avec l'ensemble des acteurs de l'hôpital à partir de l'outils *Kahoot* [267].
- Dépouillement de la boîte à idées et affichage des meilleures idées sur les stands.

[267] Kahoot est une application en ligne permettant de générer des QCM interactifs. Ces derniers, utilisés sur tablette, iPhone ou ordinateur, donnent la possibilité aux joueurs de s'autoévaluer, tout en visualisant en direct leur degré de réussite ainsi que celui de leurs concurrents. https://kahoot.com/

➔ *SUPPORT DE COMMUNICATION*

Le choix s'oriente vers la création de supports de communication ludiques, comme :

- Affiches : Une affiche par thème (voir sur les plateaux-repas à la cafétéria, dans les services et les ascenseurs) et une affiche qui récapitule l'ensemble des thématiques[268],
- Sites web (voir Annexe n°14 page 189)
- Vidéos : 1 vidéo par thématique (exemple Protéger sa vie privée en 6 étapes[269],
- Intranet : Info flash sur la première page et plus de détails sur la rubrique dédiée.
- Brochures et prospectus : Brochure reprenant toutes les thématiques abordées dans le mois
- Gadgets : Badges, stylos, autocollants, éphéméride (1 jour = 1 conseil), clef USB sécurisée,…
- Création d'un logo « Protecteur de l'info », « Protégeons nos infos », etc.
- Privilégier l'effet de surprise ! C'est le mois blanc : le fond d'écran du bureau des ordinateurs blanc de tous les postes de l'hôpital sera modifié avec la thématique de la semaine.

➔ *RESSOURCES ET PILOTAGE*

- Le représentant des usagers,
- Sophos (fournisseur d'antivirus) Nicolas Audry. Financement des gadgets et présence d'un stand sur une journée.
- ANSSI (représentant local)
- La gendarmerie (représentant local)
- Le service juridique de l'hôpital,
- Le Data Protector Officer (DPO), garant de la mise en place du RGPD,
- Le Responsable de la Sécurité du Système d'Information (RSSI),
- La Directrice du Système d'Information de l'Organisation (DSIO) de l'établissement,

➔ *ACTIONS PONCTUELLES DEJA LANCEES ET ETOUR D'EXPERIENCE*

- Envoi de courriels de sensibilisation « opportunistes », en cas d'identification d'un sujet ou d'un événement sur lequel communiquer a été adressé par courriel à l'ensemble des acteurs de l'hôpital.
  - Les messages opportunistes diffusés sur l'intranet sont lus, suivant les sujets d'actualité (mise en garde sur les virus en cours, les campagnes de phishing, etc.). Les utilisateurs ont régulièrement des questions complémentaires se rapportant à leur outil de travail ou leur sphère personnelle (comment protéger mon ordinateur familial). Ce média permet d'être présent régulièrement (l'intranet est la page d'accueil de l'explorateur Web).
- Diffusion de messages sur le portail de sensibilisation « opportunistes », en cas d'identification d'un sujet ou d'un événement sur lequel communiquer,
- Diffusion de messages sur le portail de sensibilisation « opportunistes », en cas d'identification d'un sujet ou d'un événement sur lequel communiquer,
  - Les utilisateurs sont demandeurs d'information au vu du nombre de message et d'appels qui sont adressés au support informatique. Une dizaine d'appels mensuels est traitée par le support informatique suite à la réception de courriels soupçonneux.
  - Les points traitants de la messagerie ont été abordés lors de discussions informelles avec la Direction des achats, des finances, de la communication et le DPO avant d'être validé comme sujet de la campagne.

---

268 Exemple https://www.ssi.gouv.fr/agence/cybersecurite/mois-de-la-cybersecurite-2018/

269 Exemple https://www.youtube.com/watch?v=U7xOBOnQ0G4

- Les sujets choisis se basent sur le retour d'expérience de RSSI et d'acteurs des organisations (voir §2.4 page 63), de la campagne des Hôpitaux du Groupement hospitalier de territoire de Saône et Loire Bresse - Morvan (page 162) et de la société Carmignac (§5.4.5 page 169).

5.4.5. GESTIONNAIRE DE FONDS SOCIETE CARMIGNAC

➔ *OBJECTIFS*

Monsieur Kelles, a défini, en accord avec le Managing Partner les objectifs de la sécurisation des informations de la société Carmignac :

- Préciser clairement les enjeux de sécurité du système d'information afin de valoriser la démarche sécurité,
- Définir l'organisation de la sécurité du système d'information en précisant les rôles et responsabilités de chacun.
- Expliciter les grands principes fondateurs
- **Des facteurs clés de succès ont été identifiés :**
  - La production de documents de haut niveau avec l'absence de vocabulaire d'expert et de détail sur les règles de mise en œuvre,
  - La rédaction de documents pérennes, avec l'absence de solution précise et de technologie, adaptable aux changements d'organisation,
  - La mise ne place de documents pragmatiques et applicables afin d'assurer l'adaptation des mesures à l'organisation et à la stratégie de l'entreprise.

➔ *SYNTHESE DU PLAN DE SENSIBILISATION*

Un plan d'action a été établi après une analyse et un accompagnement de la société WavesStone.

Une identification du niveau de maturité des populations sur les différents sujets sera effectuée en amont du projet.

Le périmètre d'application de la sécurisation de l'information a été identifié concerne :

- Tous départements et sites de Carmignac Gestion
- Les fournisseurs de prestations dans le domaine des Systèmes d'Information
- Les données dématérialisées et traitements des informations
- Les éléments techniques matériels ou logiciels
- Les infrastructures

Pour chaque acteur, des thèmes, en plus du tronc commun seront abordés :

CIBLES	ACTIONS
Tous les collaborateurs	- Bonnes pratiques à adopter & règles de sécurité - Enjeux de la protection des documents / donnée - Bonnes pratiques de sécurité, en lien avec les actualités - Bonnes pratiques à adopter & règles de sécurité - Enjeux de la protection des documents / données
Top management	- État de la menace - Rôles et responsabilités - Classification et protection des données sensibles - Continuité d'activité
Commerciaux	- Règles à respecter en situation de mobilité
Populations métier sensibles : MOA, Trading Desk, Fund Management, Reporting, Technology	- Enjeux métiers spécifiques - Classification et protection des données sensibles

CIBLES	ACTIONS
Support Fonctions	
Acteurs du PCA	- Rôles et responsabilités en cas de PCA / crise
Comptabilité	- Mesures de réduction des risques de fraude au président
Core Technologies	- Usage raisonné et protection des accès privilégiés aux SI
Office management	- Mesures de réduction des risques liés à l'ingénierie sociale

ID n° 85 les thèmes de la campagne

➔ SUPPORTS DE COMMUNICATION

L'ensemble des supports de communication sera utilisé suivant leur efficacité attendue et les coûts engendrés. L'évaluation des coûts et efficacité indiquées par la société Wavestone sont retenues comme point d'évaluation budgétaire (voir le détail §4.3 page 133).

➔ BUDGET PREVISIONNEL

Une évaluation des coûts a été fournie par la société Wavestone sur les sociétés proposant des solutions de formation en ligne (voir §4.3 page 133) et budgétaire prévisionnel a été proposée à la Direction avant la mise en place de la campagne :

CHARGES ANNEE 1	CHARGES ANNEES SUIVANTES
85 J.H. + 10 000 € 350 heures pour les participants, soit un peu plus d'une heure en moyenne par participant	57 J.H. + 10 000 € 350 heures pour les participants, soit un peu plus d'une heure en moyenne par participant

Voir le détail Annexe n°26 page 213.

➔ RESSOURCES ET PILOTAGE

- Le RSSI du cabinet,
- Services internes du cabinet afin d'éviter des coûts supplémentaires (technique et communication),
- Prestataires externes pour des actions ponctuelles (*WaveStone* et *Digital Security Econocom*[270]).

➔ ACTIONS PONCTUELLES DEJA LANCEES

Monsieur Keles a mis en place les actions suivantes pour sensibiliser les acteurs de l'entreprise :

- Campagne de courriels
- Des plaquettes de sensibilisation sur différents thèmes, sont diffusées sur les écrans de télévision de l'ensemble des sites distants et sous forme d'affiche papier format A3 dans les points les plus fréquentés (cafétéria, salle de pause, reprographie, etc.…). Ces messages ont vocations à être renouvelés tous les 2 mois (voir 0page 215),
- Ces plaquettes sont rédigées en français et en anglais, car le cabinet est international.

➔ RETOUR D'EXPERIENCE

Quelques utilisateurs prennent le temps de lire les conseils, et se montrent curieux en posant des questions à Monsieur Keles. Mais globalement, les utilisateurs montrent peu d'intérêt malgré les effets visuels des supports diffusés.

Monsieur Keles nous fait un retour d'expérience après un an de mise en place de la campagne de sensibilisation à la protection de l'information :

> *Ce que je constate concernant la sensibilisation, est le fait que l'utilisateur va montrer de*

[270] Digital.Security a été fondée en 2015 par un groupe d'experts de la sécurité informatique et avec le soutien du groupe Econocom https://www.digital.security/fr/prestation-formation-sur-mesure

> *l'intérêt à ces sujets de sécurité :*
>
> *- À la suite d'une mauvaise expérience personnelle (phishing, virus, ransomware),*
>
> *- Lorsqu'il perd des privilèges auxquels il avait droit jusqu'ici. Cela a fonctionné lorsque nous avons verrouillé tous les ports USB par exemple.*
>
> *Je pense que pour sensibiliser un utilisateur il est préférable de lui montrer que ses données personnelles sont en danger sur internet. Surtout si son cyber comportement n'est pas correct et s'il fait preuve de peu de vigilance.*
>
> *Les utilisateurs montrant le plus de curiosité vis-à-vis de la cybersécurité sont ceux qui sont déjà sensibilisés dans leurs environnements personnels.*
>
> *La digitalisation de l'ensemble des services (banques, services publics, etc.) devrait les pousser à se montrer plus vigilent et à transposer cette vigilance dans le contexte de l'entreprise.*
>
> *Pour cela un coup de pouce de l'état et des médias sont la bienvenue afin d'attiser leurs curiosités.*

5.5. CONCLUSION

Qu'elles sont les conditions de la réussite du projet de sensibilisation à la protection de l'information ? :

ACTIONS	DETAILS
Entreprendre un état des lieux	Entreprendre un état des lieux de la situation actuelle (risques et menaces), est la première chose à évaluer afin de bien connaître les impacts sur l'organisation, les équipements présents sur le site, mais aussi et surtout de connaître les comportements des utilisateurs.
Se fixer des objectifs	Des objectifs SMART (Spécifique, Mesurable, Ambitieux, Réaliste, Temporel) seront mis en place, tout en gardant à l'esprit les actions possibles à long terme.
Indicateurs de suivi	Définir des indicateurs de suivi. Ils permettront par la suite d'évaluer les effets de la campagne de sensibilisation.
Méthodes	Analyser et améliorer un processus nécessite de questionner ceux qui ont l'expérience de son fonctionnement réel. Les méthodes de DesignThinkink, Genba Walk inspirerons notre approche en favorisant l'activité sur le terrain. Le « Patient traceur » (voir §5.4.2 page 154) sera utilisé en milieu hospitalier,
Formation des adultes	Comprendre et maîtriser la formation dispensée à des adultes. L'approche de la formation des adultes est différente de celle des enfants (andragogie à l'opposé de la pédagogie - §3.2.4 page 86)
Métiers de l'organisation	Comprendre les métiers de l'organisation, leur processus afin d'adapter les messages et les actions à leurs préoccupations. Exemple une formation en présentielle sera difficile à mettre en œuvre pour une population de commerciaux en déplacement permanent…,
Sectoriser les acteurs à sensibiliser	Le top management a des préoccupations différentes des personnes qui gèrent les données comptables par exemple. La disponibilité d'un Directeur est contrainte par rapport à un employé comptable… Exemple de sectorisation dans un établissement de santé : personnel soignant, direction et cadres supérieurs, personnel administratif et technique, corps médical, équipes DSI et administrateurs techniques, fonctionnels et biomédicaux.
Valoriser	Reconnaître et valoriser constamment les actions accomplies par les acteurs de l'organisation.
Engagement	Mettre en place un mode de fonctionnement qui favorise un engagement Exemple : mise en avant des personnes ayant déjoué des pièges d'atteinte à l'information dans le journal de l'organisation,
Qualité de la communication	Accorder une attention particulière à la qualité de la communication, en appliquant des techniques professionnelles respectées par les agences de

ACTIONS	DETAILS
	communication (comment rédiger un message la construction d'une documentation, l'impact de messages, l'influence des couleurs) en collaborant avec le responsable de la communication ou un prestataire externe,
Inventifs et ludiques	Être inventifs et ludiques afin de capter l'attention des acteurs de l'organisation, qu'ils adhèrent à la politique de la protection de l'information mise en œuvre, soient moteurs et fassent naturellement du prosélytisme,
Études de coût/rentabilité	Effectuer des études de coût/rentabilité des supports utilisés, à l'instar d'une étude « rapport qualité/prix » afin de choisir des outils qui impacteront un maximum de personnes au moindre coût tout en étant de qualité et faire des choix en toute connaissance de cause (exemple du paquet de post-it et du calendrier),
Outils	Proposer des outils professionnels, parfois gratuits, pour tous les budgets. Nous savons que la sécurité du système d'information est, dans la majorité des cas, sous-dotée et que les RSSI doivent, se « débrouiller » pour mener une campagne de sensibilisation. Cette réflexion ressort des interviews menées et lectures d'organisation spécialités dans la sécurité[271][272][273],
Mesurer	Mesurer « la sensibilisation apportée » et adapter les outils en conséquence ou en changer, Suivre les indicateurs de résultats est indispensable pour le pilotage de l'action et pour l'implication du personnel. Il s'agit d'outils permettant de parler le même langage et de se référer à des éléments lisibles et bien définis.
Plaisir	Enfin, bannir les actions contraignantes et ennuyeuses et favoriser les outils ludiques et actions provoquant du plaisir (Exemple : concours avec lots à gagner…) et la cohésion de groupe et l'appartenance à l'organisation.

ID n° 86 tableau de conclusion

[271] Article : étude KPMG, « Les établissements de santé : en l'espace d'un an, et malgré une actualité forte et anxiogène la cybersécurité est passée de la première à la cinquième place des priorités des organisations » http://itsocial.fr/metiers/direction-generale/pdg-ont-chemin-a-faire-de-prendre-cybersecurite-serieux/

[272] Cybercriminalité : l'insuffisante prise de conscience des pouvoirs publics http://www.lefigaro.fr/vox/societe/2017/05/19/31003-20170519ARTFIG00272-cybercriminalite-l-insuffisante-prise-de-conscience-des-pouvoirs-publics.php

[273] « La sensibilisation peut coûter des centaines de milliers d'euros » Guillaume Laudière, consultant sécurité chez Devoteam http://bfmbusiness.bfmtv.com/01-business-forum/comment-sensibiliser-les-salaries-a-la-securite-informatique-564825.html

CONCLUSION

« Face au monde qui change, il vaut mieux penser le changement que changer le pansement ! »
Francis Blanche[274]

[274] Francis-Jean Blanche, dit Francis Blanche, auteur, acteur, chanteur et humoriste français décédé.

Nous ne conduisons pas une voiture tous feux éteints et sans permis sur une autoroute ! C'est le meilleur moyen d'avoir un accident et/ou se faire arrêter par les gendarmes ! Le point numéro un sera donc, de faire passe ce fameux permis « cyber protection » aux acteurs de l'organisation en leur donnant les éléments nécessaires.

Nous leur donnerons tous les exemples utiles pour qu'ils connaissent leurs ennemis et comprennent de quoi les pirates informatiques sont capables.

Il n'existe pas de campagne de sensibilisation miracle ou unique !
mais des campagnes différentes adaptées à
l'organisation et aux acteurs qui la composent.

Les réponses apportées par les professionnels, les quidams et le retour des personnes qui ont participé à la construction des campagnes sont éloquentes : chacun à « sa » recette qui fonctionne dans son secteur d'activité. Il apparaît qu'un mixte d'outils ou d'actions est nécessaire pour marquer les esprits.

Le point noir d'un grand nombre de protecteurs de l'information est le manque de budget (voir les retours d'expérience au §2.4 page 63), la question à se poser est :

Vaut-il mieux faire avec les moyens du bord
ou attendre un hypothétique budget ?
La première réponse est évidemment la bonne !
cela n'empêche pas de demander le budget…

Les cybers attaquants n'attendront pas que nous ayons un budget pour s'attaquer à l'organisation par l'intermédiaire des acteurs de l'entreprise. Ils profiteront surtout de l'ignorance de ces derniers pour nous soutirer de l'argent et nous faire subir d'autres vilenies entraînant la fermeture de l'entreprise !

Des supports de communication gratuits se trouvent à foison sur internet (voir Annexe n°14 page 189) et **l'ingéniosité et l'imagination du protecteur de l'information n'ont pas de prix !**

Tous les supports disponibles sont à squatter pour communiquer : coin café, intranet, télévisions internes, self, etc., les acteurs sont demandeurs d'information.

La difficulté se trouve ailleurs :
Capter l'attention ! Susciter l'intérêt ! Mener le changement !

La conduite du changement avec **ADKAR** en respectant l'équation du changement avec l'andragogie (transposition dans l'univers de l'apprenant). La sphère privée est une cible à exploiter : l'apprenant sera amené sur son terrain personnel afin de le toucher au cœur (son compte en banque, le partage de l'ordinateur familiale), son orgueil pourra être titillé (ses enfants sont parfois mieux informés des dangers de l'internet).

Montrer les choses par des illustrations plutôt que de les expliquer par des mots comme le préconise le **Design Thinking.**

La projection mentale est intéressante : des images pourront être imprégnées dans l'esprit des acteurs comme l'usage d'un password unique comparé à une clef qui ouvrirait l'ensemble des

portes de la maison, de la voiture… La clef est volée ou perdue et c'est la catastrophe.

Le **PEI -Programme d'Enrichissement Instrumental- et l'andragogie** : Considérer l'acteur de l'organisation pour ce qu'il est, avec son potentiel d'apprentissage et pas comme nous souhaiterions qu'il soit. Comprendre ses problématiques afin de le guider vers la connaissance tout en corrigeant ses erreurs au fil de sa progression.

Heutagogie, andragogie et PEI : Donner des outils de l'autonomie adaptés à leur vie dans l'organisation et les contraintes de celle-ci avec les serious game et la formation en ligne, responsabiliser et faire confiance aux apprenants.

Genba Walk : Aller au-devant des acteurs de l'entreprise, dans leur écosystème, recueillir des faits à utiliser en campagne de sensibilisation.

La démarche des parcours permet de se positionner sur le terrain afin de recueillir des exemples concrets dans lesquelles les acteurs se reconnaîtront durant les campagnes et provoquer des situations chocs qui marqueront les esprits.

Le protecteur de l'information profitera de toutes les rencontres (réunion, pause-café, déjeuner…) pour écouter les remarques des acteurs de l'organisation afin de comprendre leurs problématiques (« en voyage, le VPN ne marche jamais alors je vais au wifi du bar de l'hôtel ! »)..

Les actions coup de poing sont parfois nécessaires pour arriver à ses fins !

Les acteurs sont, en général de bonne foi et demandeurs d'action de sensibilisation comme nous l'avons constaté lors de la validation des actions exposées plus haut.

La Direction est motrice de la sensibilisation si nous lui expliquons les enjeux à partir de faits. La sensibilisation du Top management commence peut-être pas là !

Un humain est heuristique par nature !
Les humains ont un cerveau : utilisons-le ![275])

Les compléments techniques sont nécessaires à la protection de l'information, mais nous pouvons convenir qu'un humain est plus intelligent qu'un antivirus ? !

Et si on se positionnait sur le point économique !

Les chefs d'entreprise ont la responsabilité de leur outil de travail où ils y passent une bonne partie de leur vie par passion, devoir ou nécessité. Les acteurs de l'entreprise, qui contribue à la pérennité de cette entreprise peuvent tout faire basculer par un mauvais clic !

Qui est responsable ? Le chef d'entreprise qui ne protège pas ses informations ou alors le salarié qui n'aura pas été formé ? Qui est le chef dans l'histoire ?

C'est un devoir économique de protéger le capital informationnel de l'organisation tout autant pour les PME que les grandes entreprises. La fuite de brevets, de données sensibles est un crime si on joue à l'autruche. Les WannaCry and Co ont bloqué des entreprises, des hôpitaux et causés

[275] Jean Capron « Inclure les humains dans la cyberdéfense pour protéger notre business » Ambassade de Grande-Bretagne 20 septembre 2016

des dégâts financiers énormes (voir 1.6.1 page 42). Le pirate informatique ne fait la fine bouche et cible tout ce qui pourra lui rapporter de l'argent.

« Technique or not technique ? »

Nous l'aurons compris durant l'analyse des réponses apportées par les professionnels, les quidams, les actions menées sur le terrain et les réflexions tout au long du mémoire : **le protecteur de l'information ne sera pas une personne technique.**

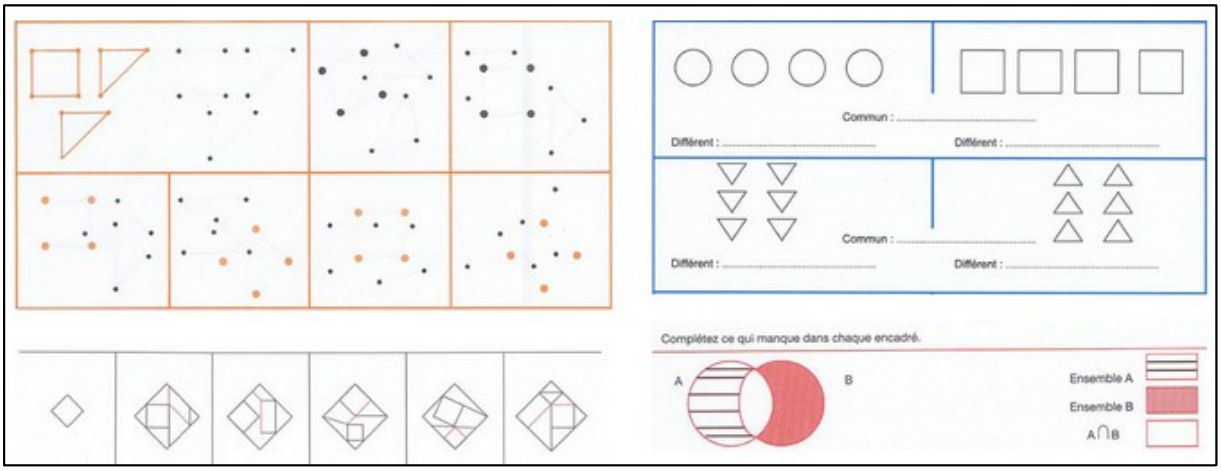
Le message à faire passer n'est surtout pas technique, l'acteur qui se retrouvera en face de nous souhaite savoir comment ne pas tomber dans un piège et se moque éperdument de connaître le fonctionnement du pare-feu !

Pour conclure, nous garderons à l'esprit que le but de la sensibilisation est de :

Transformer, l'humain d'ennemi potentiel, en allié de la protection de l'information

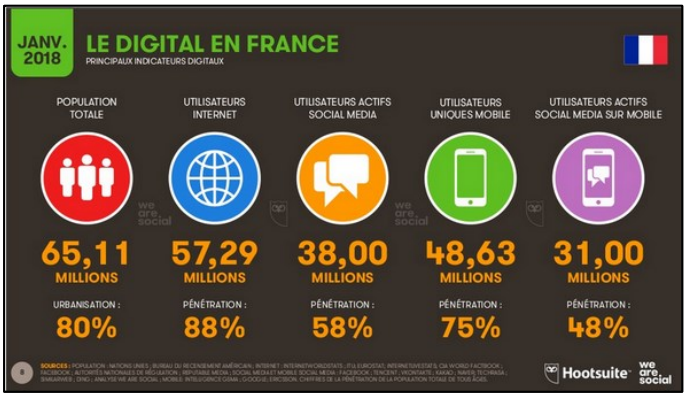
ANNEXES

Annexe n°1 Exemple d'outils de la méthode PEI de Reuven Feuerstein



ID n° 87 Exemple d'outils de la méthode PEI de Reuven Feuerstein source https://3-bis.fr/quest-ce-que-la-methode-feuerstein/

Annexe n°2 Usage du digital en France en janvier 2018.



ID n° 88 usage du digital en France en janvier 2018 source Hootsuite

Annexe n°3 Prévisions des cybers menaces 2018

PROOFPOINT[276], PROPOSE UN RAPPORT TRIMESTRIEL. IL RESSORT DU 4E TRIMESTRE 2017 :

- Attaques par courrier électronique : le volume de messages comportant des pièces jointes malveillantes a bondi de 300 %. Une hausse moindre qu'au trimestre précédent qui avait établi un record avec 600 % d'augmentation ! Et plus de 2 200 % par rapport au troisième trimestre 2016.
- Les ransomwares : Comme au trimestre précédent, ils représentent la première catégorie de logiciels malveillants avec 57 % du volume total des attaques par courriel. Les attaquants fixent de plus en plus souvent des rançons en dollars américains ou en monnaie locale (bien que le paiement lui-même soit généralement toujours effectué en crypto monnaie).
- Les chevaux de Troie bancaires : THE TRICK reste le cheval de Troie bancaire le plus utilisé. Il représentait 84 % de tous les pourriels malveillants contenant un cheval de Troie bancaire (70 % au trimestre précédent.)

[276] Proofpoint est une entreprise spécialisée en cybercriminalité basée à Sunnyvale, California

- Réseaux sociaux : Le nombre de comptes frauduleux de services clients sur les médias sociaux a augmenté de 30 %. Parallèlement, les liens d'hameçonnage dans les médias sociaux ont augmenté de 70 % par rapport au trimestre précédent.[277]

ÉDITEURS D'ANTIVIRUS KASPERSKY[278] ET SYMANTEC,

- Les particuliers devront redoubler de vigilance et changer leur comportement, notamment face à l'essor de l'IoT (§Annexe n°1 page 179). Pour les entreprises, leur vigilance portera sur la mise en place de sécurité SaaS[279] et IaaS[280] et le renforcement de la sécurité.[281]

THREATMETRIX

- Pascal Podvin, Senior Vice-Président Field Operations chez *ThreatMetrix*[282] livrent leurs prévisions 2018 :
- La transformation digitale enflammera, et mettra en danger, les nouvelles industries.
- Les cybercriminels ont dérobé 35 000 dollars par minute aux institutions financières au cours des six dernières années. Nos recherches ont confirmé une augmentation de 240 % des créations frauduleuses de comptes au cours du troisième trimestre 2017 comparé à la même période en 2015, 2018 sera probablement témoin d'une combinaison de cyber fraudes et d'arnaques financières traditionnelles, comme l'utilisation de passeurs d'argent (ou « monnaie mules[283] »).
- Les objets connectés formeront « L'Internet des Menaces ».
- La mise sur le marché de nombreuses identités volées en 2017, va faire diminuer les tarifs ; par exemple le prix d'une carte de crédit pourrait tomber à moins d'un dollar en 2018.
- Nos dernières statistiques indiquent que le volume de cyberattaques identifiées en 2017 a été généré par la dissémination rapide de données d'identification volées.
- Près d'un milliard de personnes n'ayant jamais eu de compte bancaire, se retrouveront prochainement à gérer l'intégralité de leur vie financière sur leur téléphone mobile, sans comprendre les dangers que représentent les attaques de phishing et autres formes de fraudes.
- Le cyber crime continuera de profiter au terrorisme.

Annexe n°4 Délai de détection des incidents

L'incident le plus difficile, le plus long à détecter et à contenir est le piratage criminel (323 jours). Les violations de données causées par des erreurs humaines et des problèmes techniques prennent moins de temps à être identifiées et à contenir (257 jours et 271 jours, respectivement).

277 Source : https://secureidees.com/?p=6388

278 Kaspersky Lab. est une société privée spécialisée dans la sécurité des systèmes d'information proposant des antivirus, anti-spyware, anti-spam ainsi que d'autres outils de sécurité. Elle a été fondée par Natalya Kasperskaya et Eugène Kaspersky en 1997 et son siège est à Moscou, Russie.

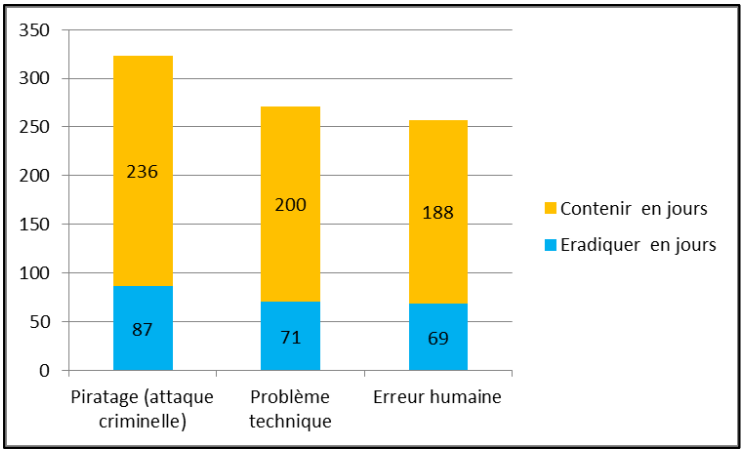
279 Le logiciel en tant que service ou software as a service (SaaS)

280 L'infrastructure en tant que service ou, en anglais, infrastructure as a service (IaaS)

281 Source : https://secureidees.com/?p=5604&

282 Spécialiste de l'identité digital https://www.threatmetrix.com/fr/

283 Les « money mules » sont recrutées sur internet comme agents financiers par des organisations criminelles dans le but de blanchir de l'argent sale. Cet argent provient notamment du trafic de drogues, du trafic d'êtres humains et d'escroqueries sur internet. Toute personne qui met son compte à disposition pour transférer de l'argent sale peut être accusée de complicité de blanchiment.



ID n° 89 piratage et détection

Annexe n°5 Le comportement humain (source de failles) : Les états

L'élection présidentielle française, de 2017, a été la victime d'une attaque massive et coordonnée contre l'équipe de campagne du président Emmanuel Macron. La diffusion massive sur internet de documents volés, parmi lesquels figuraient des faux, avait pour intention d'influencer les résultats de l'élection[284].

Le mouvement « *Umbrella revolution* [285] » a fait l'objet d'une attaque virulente DDoS en juin 2014. Les mêmes protestataires avaient été victimes d'une campagne visant leur téléphone portable[286]. La même année, la Tunisie a elle aussi, été victime d'une attaque DDoS à l'encontre de son système d'enregistrement des électeurs.

Pour clore l'année 2014, riche en attaque contre les institutions, le site de la commission centrale des élections en Ukraine, a été la cible du groupe de cyber activisme appelé *CyberBerkut*[287]. Ce groupe est connu pour d'autres méfaits à l'encontre des autorités ukrainiennes et de l'OTAN.

Plus proches de nous, plusieurs partis politiques, particulièrement les démocrates, en lice pour la campagne électorale américaine ont été piratés par des pirates informatiques russes[288]. Afin de sensibiliser les partis politiques français, le Secrétariat général de la défense et de la sécurité nationale (SGDSN) a organisé[289] au mois d'octobre 2016 une campagne de sensibilisation sur ces cyberattaques.

---

284 Cybercriminalité : l'insuffisante prise de conscience des pouvoirs publics http://www.lefigaro.fr/vox/societe/2017/05/19/31003-20170519ARTFIG00272-cybercriminalite-l-insuffisante-prise-de-conscience-des-pouvoirs-publics.php

285 Umbrella revolution : mouvement protestataire à Hong Kong réclamant des élections locales

286 https://www.interieur.gouv.fr/content/download/101311/797853/file/Etat-de-la-menace-Janvier-2017.pdf

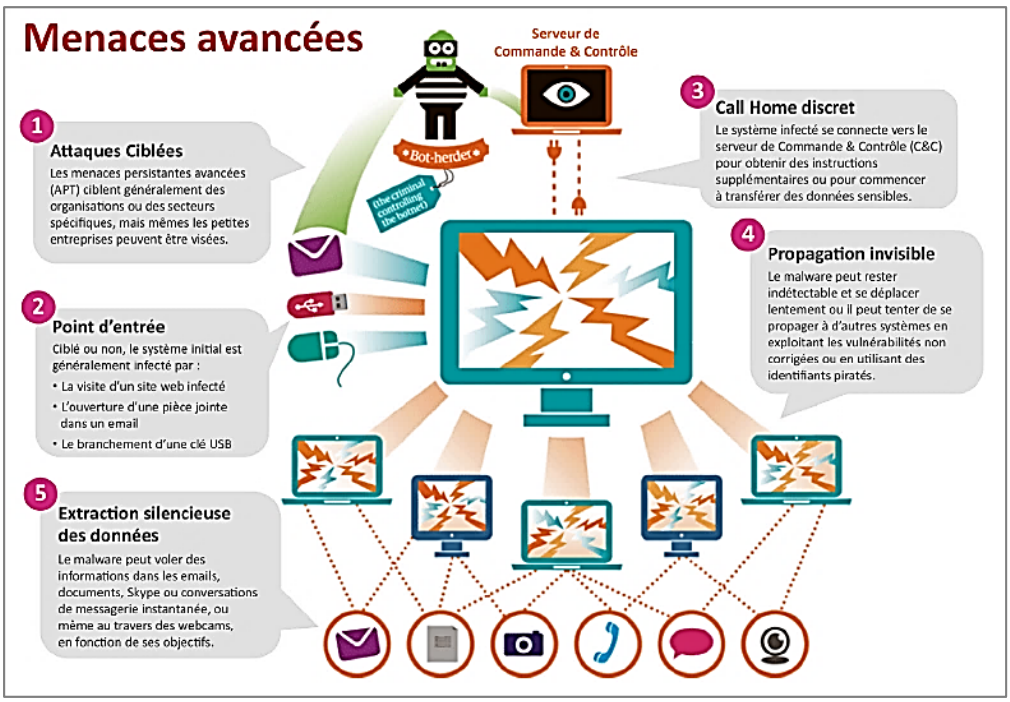
287 Les CyberBerkut est un groupe d'hacktivistes luttant contre le pouvoir ukrainien. Formé en 2014, après la dissolution des forces spéciales de la police « Berkut ».

288 http://edition.cnn.com/2016/06/21/politics/dnc-hack-russians-guccifer-claims/

289 http://www.lemonde.fr/pixels/article/2016/12/21/des-attaques-informatiques-a-visee-politique-envisageables-en-france_5052650_4408996.html

Annexe n°6 Résumé des scénarios classiques d'attaques

Les motivations principales des pirates informatiques sont [290] :



ID n° 90 scénario d'attaque classique (source : Sophos)

Annexe n°7 Dispositifs médicaux

STIMULATEURS CARDIAQUES

Les attaques contre les dispositifs médicaux augmentent, car ceux-ci comportent des « portes dérobées » ou des possibilités d'accès à distance non sécurisés, par lesquels les cybers attaquants s'introduisent dans les appareils. [291] Un grand nombre de ces appareils fonctionnent avec une version de Windows dépassée qui est ignorée des logiciels de sécurité [292].

Des failles de sécurité ont été révélées en 2017 sur des appareils médicaux, tels que les stimulateurs cardiaques [293] ou les pompes à insuline[294]. (Voir §1.3 page 18)

Cette liste n'est pas exhaustive elle a le mérite, d'attirer l'attention sur la dangerosité de ces appareils si ceux-ci sont insuffisamment sécurisés.

Sergey Lozhkin, expert en sécurité chez Kaspersky Lab., a démontré comment il est facile pour les pirates informatiques de compromettre les dispositifs médicaux et les infrastructures de soins de santé [295].

---

290 « Cyber malveillance : ça n'arrive pas qu'aux autres », Cybermalveillance.gouv.fr

291 Etude de la société *TrapX Security* sur les cyber-attaques dirigées et détectées par les établissements de santé entre fin 2015 et début 2016 https://securityledger.com/wp-content/uploads/2015/06/AOA_MEDJACK_LAYOUT_6-0_6-3-2015-1.pdf

292 Etude de la société *TrapX Security* sur les cyber-attaques dirigées et détectées par les établissements de santé entre fin 2015 et début 2016 https://securityledger.com/wp-content/uploads/2015/06/AOA_MEDJACK_LAYOUT_6-0_6-3-2015-1.pdf

293 https://threatpost.com/fda-recalls-465k-pacemakers-tied-to-medsec-research/127750/

294 http://thehackernews.com/2017/09/hacking-infusion-pumps.html

295 http://securityaffairs.co/wordpress/44558/cyber-crime/hack-medical-devices.html

La FDA (Food and Drug Administration)[296] a prouvé, grâce à des tests que les stimulateurs cardiaques développés par la société Saint Jude Medical pouvaient être piratés à distance, et qu'il était possible de prendre le contrôle du stimulateur cardiaque en modifiant le rythme cardiaque du porteur, ou d'épuiser la batterie. Le micrologiciel pilotant le stimulateur cardiaque en était la cause. 500 000 Américains ont été concernés par cette faille de sécurité.[297]
Deux pirates informatiques, lors de la conférence Black Hat 2018[298] ont démontré, en directe la possibilité de pirater un stimulateur cardiaque (de la marque Medtronic) et lui implanter un logiciel malveillant. Cette attaque peut épuiser les piles de l'appareil et aussi envoyer une décharge mortelle au patient.
Cette démonstration a pour but de mettre en lumière le laxisme de certains fabricants, qui ne font rien pour remédier à ces failles de sécurité. Les chercheurs Billy Rios de la société de sécurité *Whitescope* et Jonathan Butts de QED Secure Solutions ont averti le fabricant des failles potentielles de leur appareil en 2016. Cette société a mis 10 mois pour consulter les conclusions de ces deux chercheurs et à déclarer que « *Ces résultats n'ont révélé aucun nouveau risque potentiel en matière de sécurité. Les risques sont contrôlés et le risque résiduel est acceptable* ». Les programmateurs de cette société utilisent le système d'exploitation Windows XP pour gérer les appareils ![299]

POMPES A INSULINE

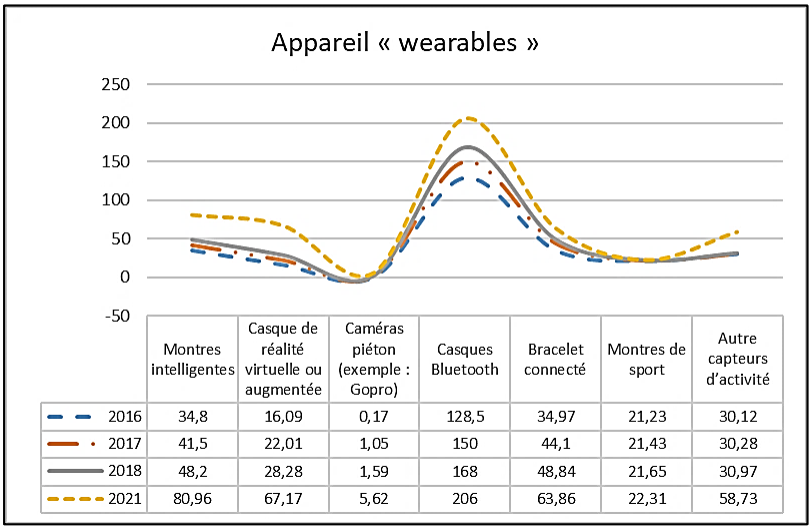
Fin décembre 2016, l'un des modèles de pompe à insuline du laboratoire pharmaceutique Johnson & Johnson présentait une vulnérabilité, qui exploitée par une personne malveillante, permettait d'injecter une dose potentiellement mortelle pour son porteur. 114 000 patients aux Etats-Unis et au Canada ont été impactés. Septembre 2017,[300] Scott Gayou[301], chercheur en sécurité, a découvert huit vulnérabilités dans la pompe à injection sans fil *Medfusion 4000*, fabriquée par Smiths Medical[302]. Les appareils sont utilisés à travers le monde pour fournir de petites doses de médicaments dans les services de soins intensifs aigus (néonatals et pédiatriques) et en salle d'opération.
Ces défaillances peuvent être exploitées par des cybercriminels afin de manipuler la pompe, ce qui pourrait provoquer une issue fatale pour le patient.
Jay Radcliffe, diabétique et chercheur en sécurité chez *Rapid7*, a prouvé que le flux de connexion de sa pompe à insuline n'était pas chiffré et par conséquent, pouvait être intercepté afin d'en modifier son intégrité.

Annexe n°8 Les IoT (Internet des Objets)

Pour le meilleur et pour le pire !
La moindre porte ouverte sera exploitée par les criminels pour s'introduire dans l'organisation, afin de la paralyser et chez les particuliers pour leur voler leurs informations personnelles.
L'attention et la sensibilisation doivent également être portées sur les autres applications connectées à

296 La Food and Drug Administration (FDA) est l'Agence américaine des produits alimentaires et médicamenteux.
297 THREATPOST « FDA Recalls 465K Pacemakers Tied to MedSec Research" 31/8/2017 https://threatpost.com/fda-recalls-465k-pacemakers-tied-to-medsec-research/127750/
298 Black Hat a été créé par le pirate informatique Jeff Moss (alias The Dark Tangent) en 1997. Un rassemblement a lieu chaque année à Las Vegas auquel participent les professionnels de la sécurité au sens large (hackers, responsables sécurité en entreprises, consultants, pentesters, universitaires, officiers d'armée, experts des agences gouvernementales, politiques, etc.…) https://www.blackhat.com/us-18/
299 WIRED "A new pacemaker hack puts malware directly on the device" 8/9/2018 https://www.wired.com/story/pacemaker-hack-malware-black-hat/
300 http://thehackernews.com/2017/09/hacking-infusion-pumps.html
301 Security Engineer chez Garmin International –Kansas (USA),
302 Spécialiste de l'équipement médical dans le Minnesota (USA)

internet et à l'organisation, comme les systèmes de vidéosurveillance, le suivi des flottes automobiles ou de camion, le suivi de personnes, la télésurveillance, les jouets, les assistants vocaux, etc.
Avec l'Internet des Objets, les « *zombies* » peuvent être de nature bien différente.



	Montres intelligentes	Casque de réalité virtuelle ou augmentée	Caméras piéton (exemple : Gopro)	Casques Bluetooth	Bracelet connecté	Montres de sport	Autre capteurs d'activité
2016	34,8	16,09	0,17	128,5	34,97	21,23	30,12
2017	41,5	22,01	1,05	150	44,1	21,43	30,28
2018	48,2	28,28	1,59	168	48,84	21,65	30,97
2021	80,96	67,17	5,62	206	63,86	22,31	58,73

ID n° 91 évolution des technologies portables (wearables).

LES BOTNETS

Un botnet[303], peut-être constitué d'autres objets infectés que des ordinateurs. Ceux-ci effectuent à leur insu diverses actions comme participer à la diffusion massive de pourriel ou à des attaques par déni de service (DDoS) distribué.
Septembre 2016, l'entreprise roubaisienne OVH[304] a subi une attaque DDoS massive de son infrastructure. Depuis le 23 septembre, plus de 1,5 terabits bombardaient chaque seconde les serveurs de OVH. Des pirates informatiques ont infiltré et contrôlées à distance, près de 150 000 caméras disséminées sur la planète, comme botnet, pour mener cette attaque.
La société Sucuri[305] a découvert un botnet, après l'attaque du site internet d'une petite bijouterie qui a été paralysé pendant plusieurs jours. Le botnet était constitué de plus de 25 500 caméras de vidéosurveillance réparties à travers le monde, principalement situées à Taïwan, aux Etats-Unis, en Indonésie et plusieurs centaines en France.

LES JOUETS

Les jouets sont également la cible des pirates informatiques. Pourquoi pirater un jouet ? Le but est d'écouter des conversations, de visualiser l'intérieur des maisons[306] à des fins malveillantes ou par simple défi et amusements !

---

303 Un botnet (de l'anglais, contraction de « robot » et « réseau ») est un réseau de bots informatiques, des programmes connectés à Internet qui communiquent avec d'autres programmes similaires pour l'exécution de certaines tâches.

304 Leader mondial de l'hébergement internet

305 Source : https://blog.sucuri.net/2016/06/large-cctv-botnet-leveraged-ddos-attacks.html

306 « Comment hacker un Furby et lui faire faire des choses terrifiantes »
https://motherboard.vice.com/fr/article/784b5y/comment-hacker-un-furby-et-lui-faire-faire-des-choses-terrifiantes
Noël connecté : sécurité des jouets connectés http://www.e-enfance.org/actualite/noel-connecte-securite-jouets-connectes.html

Annexe n°9 Les réseaux sociaux

Les réseaux sociaux, sont un des vecteurs de la communication de la société actuelle. Ceux-ci sont également ciblés par les criminels du net :

- 1er février 2013, Twitter[307] à subit une attaque de ses serveurs. Après enquête, la firme a avoué que les pirates « *ont eu accès aux données personnelles – noms d'utilisateurs, adresses courriel, mots de passe cryptées – d'environ 250 000 utilisateurs* ».
- 18 mai 2016, LinkedIn[308] a été piraté. Plus de cent millions d'identifiants, comprenant des mots de passe chiffrés, sont mis en vente en ligne. Ces informations auraient été volées en 2012 à la suite d'un piratage du réseau
- 30 mai 2016, Myspace[309], 427 millions de mots de passe, ont été mis en vente sur un site spécialisé dans le recel de données volées, la base de données entière est mise en vente pour 2 500 €, seulement !
- 12 mai 2016, Tumblr[310], 65 millions d'adresses de courriels et de mots de passe ont été volés d'après une estimation de Troy Hunt[311], chercheur en cyber sécurité, car la société ne souhaite pas communiquer sur l'incident. Troy Hunt a mis en place une plateforme pour vérifier si son adresse courriel est corrompue ou a été volée sur https://haveibeenpwned.com/.

Annexe n°10 Quelques dates notables qui ont échelonné la cybercriminalité

DATE	ÉVENEMENTS
1970	Les premiers virus sont apparus dès les années 1970, notamment Creeper. Ce virus s'introduisait, via un modem, dans un système distant. Il affichait, alors le message d'avertissement à l'utilisateur infecté : « I'm the creeper : catch me if you can ».
1971	La première attaque d'un réseau informatique a eu lieu avec l'utilisation d'un sifflet offert dans une boîte de céréales de la marque Cap'n Crunch aux USA. Le son émis par le sifflet a été détourné pour émettre des appels téléphoniques312.
1973	Un ordinateur est utilisé par un caissier d'une banque pour voler deux millions de dollars,
1975	En 1975, est apparu Pervading Animal, un jeu développé pour un Univac 1108 313. Pour l'instant, les experts n'ont pas encore défini s'il s'agissait d'un virus ou du premier cheval de Troie. (Source fr.wikipedia.org)
1981	Ian Murphy, allias « capitaine Zap » est le premier cybercriminel à être condamné en tant que tel. Il a piraté le réseau AT & AT et modifié l'horloge interne afin de réclamer des heures supplémentaires,
1982	Elk Cloner, premier virus connu, développé par un adolescent de quinze ans. Il s'est propagé à travers le monde via des disquettes et a attaqué le système d'exploitation d'Apple,
1983	Le film « War games » révèle au grand public les actions de piratages informatiques,
1986	Le congrès américain vote le « Computer Fraud and Abuse Act », qui reconnaît le piratage et le vol en les déclarants illégaux,

307 Twitter est un réseau social de micro blogage géré par l'entreprise Twitter Inc

308 LinkedIn est un réseau social professionnel en ligne créé en 2003 à Mountain View (Californie).

309 Myspace est un site web de réseautage social fondé aux États-Unis en août 2003,

310 Tumblr est une plate-forme de micro blogage créée en 2007 et permettant à l'utilisateur de poster du texte, des images, des vidéos, des liens et des sons sur son tumblelog.

311 Article paru sur motherboard, https://motherboard.vice.com/en_us/article/nz7nxx/the-rise-of-have-i-been-pwned-an-invaluable-resource-in-the-hacking-age-troy-hunt, 10/3/2016

312 John Draper, un « phone freak », découvre qu'un sifflet offert en cadeau dans des boîtes de céréales Cap'n Crunch produit les mêmes sonorités qu'un téléphone qui gère des ordinateurs en réseau. Phone phreak est un terme utilisé pour décrire les programmateurs informatiques obsédés par les réseaux téléphoniques, la base des réseaux informatiques modernes. Il construit alors une « boîte bleue » avec le sifflet qui lui a permis d'émettre des appels téléphoniques interurbains gratuits, puis a diffusé des instructions pour expliquer comment le faire.

313 Premier ordinateur traitant aussi bien des nombres que du texte commercialisé aux États-Unis en 1951. Créé par John Presper Eckert et John Mauchly, l'UNIVAC (Universal Automatic Computer) allait bouleverser le rapport de l'homme à la machine.

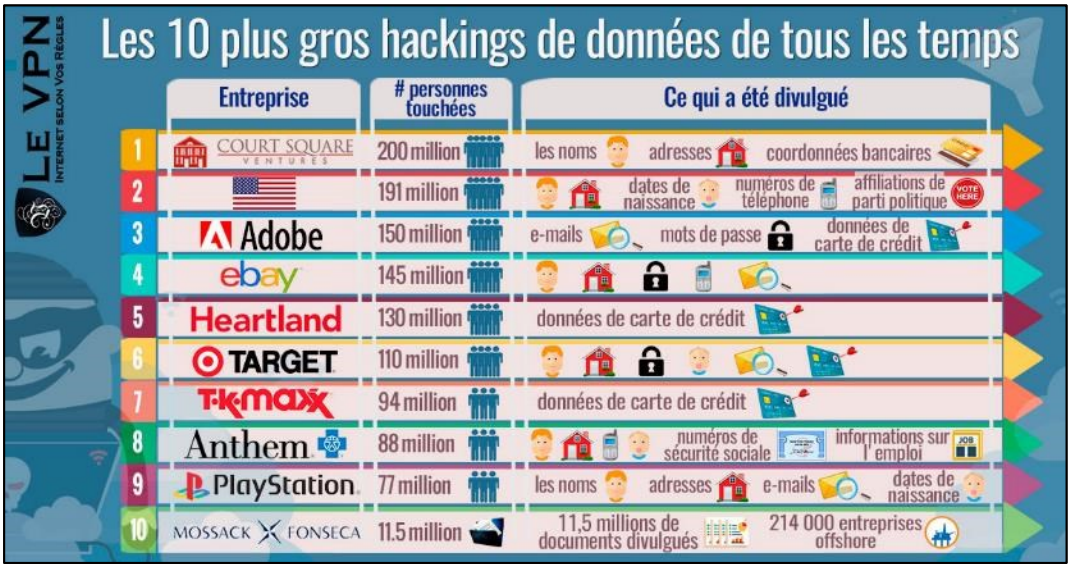
DATE	ÉVENEMENTS
1988	Robert T. Morris Junior diffuse un virus sur ARPANET, ancêtre d'internet. Arpanet était le réseau de communication interne du ministère de la défense américaine. Ce virus a infecté 600 000 ordinateurs,
1989	Le premier « rançongiciel » fait son apparition sous la forme d'un questionnaire sur le virus du sida. Nommé PC Cyborg Trojan ou encore « AIDS », ce ransomware a été programmé par Joseph Popp (biologiste anglais). 20 000 disquettes, et plus, sont expédiées à travers le monde à des industries et associations exerçant dans le secteur de la santé, parfois même luttant contre la maladie du SIDA. Le docteur Popp sera appréhendé, et indiqua qu'il voulait utiliser l'argent volé pour mener ses propres recherches contre le SIDA, ce qui n'a pas pu être prouvé.
1990	« La Legion Of Doom » et « les Masters Of Deception » sont les héritiers de John Draper. Ils mènent des actions de piratages à grande échelle des infrastructures téléphoniques aux états Unis.
1993	Kevin Poulson souhaitait gagner à un jeu téléphonique d'une radio de Los Angeles, donc il a pris le contrôle de toutes les lignes de la station. Il a été arrêté, condamné à 5 ans de prison et a été le premier criminel à être interdit d'usage d'internet en prison,
1994	Naissance du World Wide Web. Les informations et modes d'emploi de piratage sont diffusés par les cybercriminels sur le Net. La NASA, entre autres, a été piratée par un étudiant anglais avec un simple ordinateur personnel Commodore Amiga 314et un programme « blueboxing 315 » trouvé sur internet,
1995	Apparition des premiers « macrovirus » Les macrovirus sont des virus intégrés dans les applications. Ceux-ci s'exécutent au lancement de l'application (exemple : traitement de texte, les feuilles de calcul). C'est pourquoi il est dangereux d'ouvrir des pièces jointes inconnues. Les macrovirus sont difficilement détectables et constituent l'une des principales causes de piratage d'un ordinateur.
1996	Le directeur de la CIA, John Deutsch déclare que les réseaux gouvernementaux et les entreprises américains sont régulièrement attaqués. Le U.S. Government Accountability Office (U.S. GAO) a été attaqué au moins 65 000 fois avec 60 % de réussite,
1997	85 % des entreprises américaines ont été piratées et l'ignorent, suivant un rapport du FBI
1999	Apparition du virus « Mélissa » utilisant la messagerie pour effectuer des envois en masse. Il s'agit du virus le plus violent à ce jour, causant 80 millions de dollars de dommage aux réseaux informatiques. Son auteur a écopé de 5 ans de prison.
2000	Divulgation de carte de crédit des clients de CD Universal, attaques DDoS316 de AOL, Yahoo et Ebay. Le fameux virus « I love you » coure sur internet.
2001	Célèbres virus CodeRed, Nimda, Aliz, BadtransII, ILoveYou, Magistr et SirCam
2002	Le forum d'échanges entre cyber pirates « Shadow Crew » fait son apparition.
2003	« SQL Slammer » est un virus qui infecte les bases de données SQL. Il a infecté 75 000 machines en moins de 10 minutes ; c'est un record !

314 L'Amiga est une famille d'ordinateurs personnels commercialisée par Commodore International entre 1985 et 1994. Dans les années 1990, il est très populaire dans l'industrie de la vidéo.

315 Petite boîte bleu (bluebox) qui permettait de téléphoner gratuitement.

316 Attaques par déni de service

Annexe n°11 Panel d'attaques effectuées ces dernières années



ID n° 92 les 10 plus gros piratages de données de tous les temps

- *Court Ventures : Dans l'un des vols de données les plus audacieux et ayant eu le plus d'envergure à l'heure actuelle, un homme vietnamien, Hieu Minh Ngo, a été accusé d'être impliqué dans l'acquisition de millions de données sensibles sur les citoyens américains après avoir prétendu faire partie d'une société d'enquêteurs privés.*
- *Base de données des électeurs : les informations de millions d'électeurs sont devenues accessibles sur Internet aux états Unis*
- *Adobe : éditeur de logiciel*
- *eBay : sites de commerce électronique*
- *Heartland / Global Payments : entreprise de traitement des paiements. Chaque fois qu'une carte de crédit est utilisée en la glissant dans un TPE, l'information de transaction est transmise à une société comme Global Payments avant que l'information arrive à une société de carte de crédit comme Visa ou MasterCard.*
- *Target : géant américain du commerce de détail*
- *TJ/TK Maxx : chaine de magasin connue aux états Unis*
- *Assureur Santé Anthem : est le deuxième plus grand assureur santé aux Etats-Unis*
- *Réseau PlayStation : le vol atteint les consoles de jeux de Sony*
- *Affaire des Panama Papers*

Annexe n°12 Rançonnage


free

Veuillez accepter ce certificat-cadeau de 800 Euro comme notre façon de dire désolé.

RÉCLAMATION ICI

Nous nous excusons pour la mauvaise expérience que vous avez passée la dernière fois que vous achetez chez nous

ID n° 93 faux message de l'opérateur free – septembre 2017


De : Denis DEMAILLY [mailto:denissdemailly3@orange.fr]
Envoyé : mercredi 13 septembre 2017 03:57
À : Emilie.MINISINI@otenet.gr
Cc : karinesavio@aol.ch; magali.love@safti.com
Objet : TR: To.:; Prime De Fidélité

Promotions

Bonjour,
Nous entrons en contact avec vous dans le but de vous informer que vous venez de remporter le prix de" 350.000Euros.

Pour l'obtention du"Prix contacter →Monsieur HASSAN BARRY

NB: Pour plus d'infos, veuillez consulter les différentes pièces attachées en joint des renseignements détailles.

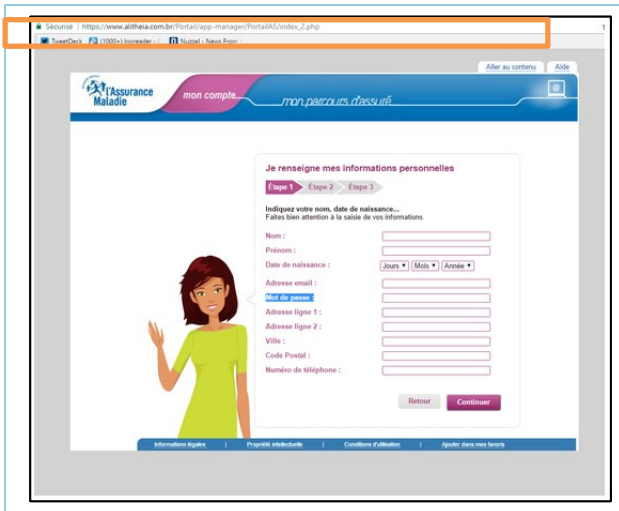
Merci de votre confiance,

En voir plus

ID n° 94 Faux courriels de l'opérateur Orange. L'expéditeur a dû se faire pirater sa messagerie – septembre 2017

Dans ce courriel il est expliqué que l'assuré est éligible à un remboursement dont le montant varie suivant le message. Le texte reproduit à l'identique un courrier légitime de la Caisse d'assurance maladie, il est donc

exempt de fautes d'orthographe qui permettaient auparavant de détecter une tentative frauduleuse.
La Caisse d'assurance maladie met en garde sur son site et donne quelques éléments permettant de se protéger. Deux éléments permettent de reconnaître les faux messages : l'absence du nom de l'assuré dans le corps du message, et le fait que les liens contenus dans le message ne renvoient pas vers le site Ameli.fr, comme le montre la barre d'adresse dans la capture d'écran ci-dessous.



ID n° 95 Faux message en provenance de la Sécurité sociale - site AMELI – mai 2017

ID n° 96 Faux courriel du service des impôts

Ils peuvent y accéder par le biais de sites Web piratés, de démos de jeux, de fichiers musicaux, de barres d'outils, de logiciels, d'abonnements gratuits ou de tout autre élément téléchargé depuis le Web sur un appareil non protégé par un logiciel anti-malware.

Annexe n°13 WannaCry

Un exemple frappant, survenu en mai 2017, démontre la fragilité de la sécurité des organisations et des établissements de santé : l'attaque « WannaCry » est à ce jour inédit. 300 000 victimes ont été répertoriées dans plus de cent cinquante pays.
Les hôpitaux sont fréquemment les cibles de ransomware :

- Des services hospitaliers du National Health Service[317] ont dû reporter des opérations chirurgicales,
- Un hôpital du Kansas aux Etats-Unis a été victime d'un ransomware le 18 mai 2016. Les ransomwares (ou "rançongiciels) sont des malwares qui paralysent un système en chiffrant l'intégralité des fichiers qui s'y trouvent. Ils proposent ensuite à la victime de lui fournir la clé qui permettra de déchiffrer ses données contre une rançon, payable en bitcoins (et donc impossible à annuler une fois payée).
- Le Hollywood Presbyterian Medical Center, un hôpital de Los Angeles, s'est retrouvé paralysé pendant 10 jours et avait dû envoyer ses patients vers d'autres établissements de santé, avait défrayé la chronique en janvier. Incapable de fonctionner normalement (ses équipes en étaient revenues au papier et au fax), il avait fini par payer la rançon de 40 bitcoins (soit environ 15 600 euros) demandée pour reprendre ses activités.

Et parmi les organisations touchées par cette attaque, on retrouve notamment Vodafone, FedEx, Renault, le National Health Service britannique ou encore la Deutsche Bahn.
La propagation s'est faite à travers des messages adressés à des milliers d'internautes de par le monde, un clic malencontreux et l'ensemble des données des ordinateurs, serveurs, robots a été mise sous contrôle des pirates qui ont réclamé une rançon pour libérer les données.

317 National Health Service, le système de santé au Royaume-Uni

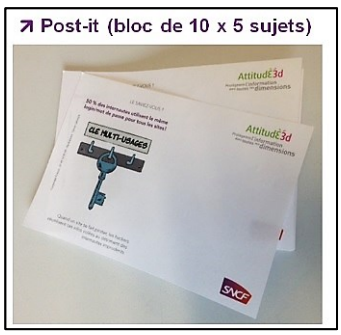
La cyberattaque globale WannaCry a causé des dégâts s'élevant à 1 milliard de dollars, relate le cabinet spécialisé « McClatchyDC ». Ces dommages ont été causés par l'immobilisation de la production de grandes organisations dans le monde entier.

ID n° 97 Message à l'écran après cryptage à la suite de l'infection

Une situation liée à la perte de donnés, à la réduction de la productivité, à des perturbations du travail, au préjudice porté à la réputation, ainsi qu'à plusieurs autres facteurs.

Annexe n°14 Support de communication

GADGETS



ID n° 98 exemple de la SNCF

SERIOUS GAMES

On commence à voir apparaître depuis quelques années les serious gaming qui sont des jeux mettant l'utilisateur dans des situations basées sur des saynètes. Ces serious game existent dans divers domaines dont la sécurité informatique.

- MAVI INTERACTIVE http://www.maviinteractive.com/ Démonstration sur https://vimeo.com/46310970
- ŒIL POUR ŒIL GAMIFICATION https://www.oeilpouroeil.fr/
- Saynètes avec quiz : CONSCIO TECHNOLOGIE https://www.conscio-technologies.com/ Démonstrations sur https://youtu.be/xWpv_yAtAYU

- Diapositive avec quiz : ELUCIDAT https://www.elucidat.com/ et BEEDEEZ https://www.beedeez.com/
- Formation en ligne spécial santé. Pour les adhérents à la centrale d'achat CAIH, réservée aux établissements de santé, un module de formation en ligne sur la sécurité du système d'information hospitalier http://www.caih-sante.org/ est proposé. La société https://www.ktm-advance.com/ est détentrice de la marche.
- Sensibiliser à la cybersécurité, le serious game CIGREF dans les entreprises https://www.cigref.fr/sensibiliser-a-la-cybersecurite-le-serious-game-cigref-dans-les-entreprises
- Netwars, la guerre sur le Net (Arte) : « Jeu documentaire » s'appuyant sur les discussions politiques actuelles entre les puissances mondiales. http://future.arte.tv/fr/netwars-la-guerre-sur-le-net-1/out-ctrl-le-webdoc
- Jeu d'influences (France 5) « La vérité c'est ce que la majorité des gens croient. » : « Jeu d'influences » propose une expérience inédite pour explorer de l'intérieur le monde de la communication de crise. En mode jeu de rôle, vous incarnez le PDG qui doit trancher sur les options de communication proposées. http://jeu-d-influences.france5.fr/
- « Profiler » un jeu sous forme d'enquête de la police scientifique (Arte) http://php4.arte.tv/forensik/profiler.html
- CCI Intelligence économique (CCI Normandie) L'organisation Zdong innovation, est menacée par une organisation mandatée par un de ses concurrents. L'organisation est dirigée par un mystérieux personnage qui dépêche ses sbires un à un, qu'il s'agira d'empêcher de nuire. http://www.jeu-ie.cci.fr/
- Cyberstrategia (Réserve Citoyenne Cyberdéfense) Inspiré du jeu de société RISK, le joueur incarne, lors d'une partie où plusieurs joueurs s'affrontent, un pays qui va utiliser (ou se protéger) des moyens d'attaques et de défense cybernétiques qui seront propre à son histoire et son modèle économique. En format jeu de rôle avec des acteurs réels, le joueur est le DSI d'une organisation internationale, dont le point est de commercialiser une application de paiement mobile avec authentification biométrique. Le projet est en phase de lancement. Vous arbitrez donc entre notre équipe interne de sécurité, vos collègues du marketing et des relations presse, et notre PDG. http://targetedattacks.trendmicro.com/fra/index.html
- Dans la peau d'un escroc (ISSA France) Détourner des millions en un coup de téléphone ? http://www.interopsys.fr/jouez-serious-game-fraude-president/
- Cryptris (INRIA) Comprendre la cryptographie. http://inriamecsci.github.io/cryptris/jeu.html
- « 2020 » est une web-série d'anticipation fondée sur un rapport de l'International Cyber Security Protection Alliance préparé par Europol et Trend Micro. http://2020.trendmicro.com/fr/
- Comprendre l'enjeu de la protection des données personnelles en s'amusant ? C'est le principe de Datak, un jeu vidéo pour navigateur qui nous plonge dans la peau d'un stagiaire fraichement recruté dans une mairie. Développé par la Radio Télévision Suisse (RTS), le jeu est disponible depuis le mois de décembre 2016 sur https://www.datak.ch/#/start
- Jeu entre un hacker et une entreprise https://www.pwc.co.uk/issues/cyber-security-data-privacy/services/game-of-threats.html
- « Keep an Eye » du Cigref. Un salarié devient l'ange gardien de son organisation et est suivi dans son privé et professionnel. Voir la bande annonce sur https://youtu.be/hITlyxBSDaI
- Autres jeux : http://www.serious-game.fr/tag/securite/

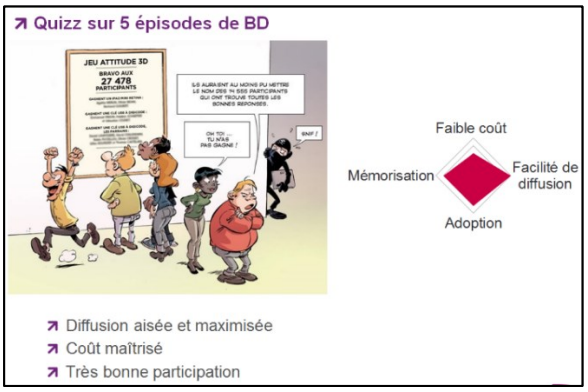
VIDEO

- https://youtu.be/ueM96CI5Y5I
- https://www.hack-academy.fr/
- Comment pirater et espionner un ordiphone à partir d'une application http://www.leparisien.fr/high-tech/video-comment-pirater-et-espionner-un-smartphone-a-partir-d-une-application-12-04-2017-6847944.php
- Conscio Technologies https://www.youtube.com/channel/UCCGp0wA7ksfbYQRUmt7ydzg
- Datak est un jeu vidéo qui propose de vous montrer différents enjeux sur la vie privée. https://www.datak.ch/#/start
- Comment protéger l'information sur les salons professionnels https://youtu.be/eLmJ_5Ev0dM

- Attitude 3d - Le programme SNCF de sensibilisation à la protection de l'information https://www.youtube.com/channel/UCC2Kui9IrKyFHnOYIY378OA/videos?view=0&sort=dd&shelf_id=0

AFFICHE

- ENISA https://www.enisa.europa.eu/media/multimedia/material/illustrations
- Poster https://www.cnil.fr/sites/default/files/atoms/files/poster_fr-optimise.pdf



ID n° 99 Questionnaire SNCF

JEUX, QUIZZ…

- CCi intelligence économique, le jeu sérieux" http://www.jeu-ie.cci.fr/
- Quizz en direct et interactif proposé par la CNIL http://incoweb.playbac.fr/indexhtml.php5?livret=72
- Jeux de rôle (http://pedagopsy.eu/jeu_de_role.html).
- Jeux interactifs : https://www.cnil.fr/fr/rentree-2017-un-nouveau-quiz-les-incollablesr-pour-sensibiliser-les-collegiens-leur-vie-privee et https://www.educnum.fr/es-tu-vraiment-incollable-sur-les-mots-de-passe
- Passer le permis web (exemple) : http://www.passe-ton-permis-web.com/

AUTRES OUTILS NUMERIQUES :

- https://kahoot.com/,
- https://quizizz.com/,
- https://www.plickers.com/
- https://dane.ac-lyon.fr/spip/Comparatif-des-outils-numeriques#,
- https://moodle.org/,
- http://numeriques.spip.ac-rouen.fr/?lang=fr
- Bases de données des durées de conservation des documents http://www.archimag.com/le-kiosque/service-web/base-de-donnees-des-durees-de-conservation-des-documents?utm_campaign_name=&uid=id_p5un0xqq7p&utm_campaign_type=&utm_campaign=
- Campagne lancée par la MGEN et la CNIL avec le célèbre Youtubeur Kevin Tran https://www.cnil.fr/fr/proteger-sa-vie-privee-en-6-etapes
- Clé de sécurité basée sur le protocole FIDO2 https://www.undernews.fr/authentification-biometrie/yubico-lance-sa-nouvelle-gamme-yubikey-5.html
- CNIL https://www.cnil.fr/fr/pourquoi-securiser-au-maximum-le-mot-de-passe-de-votre-boite-courriel
- Contenu d'une étude universitaire consacrée au droit et au numérique http://enetter.fr/
- Festival du Film Sécurité https://www.security-systems-valley.fr/festival/les-laureats
- InitiaDROIT est une association d'avocats bénévoles https://initiadroit.com/internet/
- Kit de sensibilisation https://www.cybermalveillance.gouv.fr/contenus-de-sensibilisation/
- La collection du Ceprisca http://www.ceprisca.fr/la-collection-du-ceprisca-en-libre-accesa/
- La commission européenne a lancé le projet COMPACT (COmpetitive Methods to protect local Public Administration from Cyber security Threats) pour aider les administrations publiques locales à

devenir plus cyber-résistantes https://cordis.europa.eu/ et https://www.kaspersky.fr/enterprise-security/security-awareness

- La compagnie du Hack : réseau de crowdsecurity facilite depuis 2013 la relation entre des experts en sécurité informatique et des organisations désireuses de protéger leurs patrimoines informationnels https://www.linkedin.com/company/yes-we-hack
- L'actualité sécurité informatique pour PME/PMI/TPE https://www.datasecuritybreach.fr/
- Outils pour la sensibilisation des enfants https://www.childnet.com/resources
- SecNumedu https://www.ssi.gouv.fr/particulier/formations/
- Sensibilisation et initiation à la Cybersécurité https://www.ssi.gouv.fr/uploads/2016/05/cyberedu_module_1_notions_de_base_02_2017.pdf
- Sensibilisation Sécurité information : Quelques comportements de base https://youtu.be/9r4KwAB5YxI
- Soyez acteur de la sécurité de l'information chez https://www.fun-mooc.fr/courses/unormandie/68001S02/session02/about).
- Trousse d'information Pensez cybersécurité https://www.getcybersafe.gc.ca/cnt/rsrcs/pblctns/cbrsf-tlkt/index-fr.aspx. Voir la brochure https://www.getcybersafe.gc.ca/cnt/rsrcs/pblctns/cbrsf-tlkt/cbrsf-tlkt-fra.pdf. Site https://www.pensezcybersecurite.gc.ca/index-fr.aspx
- Vis ma vie de RSSI https://youtu.be/sI9mxu8Y_Nk
- Gestion des mots de passe : https://www.cybermalveillance.gouv.fr/nos-articles/fiche-pratique-gerer-ses-mots-de-passe/ et https://www.educnum.fr/es-tu-vraiment-incollable-sur-les-mots-de-passe
- Sensibilisation des collégiens sur leur vie privée : https://www.cnil.fr/fr/rentree-2017-un-nouveau-quiz-les-incollablesr-pour-sensibiliser-les-collegiens-leur-vie-privee
- Comment espionner un téléphone intelligent : http://www.leparisien.fr/high-tech/video-comment-pirater-et-espionner-un-smartphone-a-partir-d-une-application-12-04-2017-6847944.php
- https://www.inc-conso.fr/recherche?displayModeParam=grids&keyword=&im_vid_7%5B67%5D=67

LES FORMATIONS

- CyberEdu, sensibilisation pour les formations en informatique : https://www.ssi.gouv.fr/administration/formations/cyberedu/contenu-pedagogique-cyberedu/
- SecNumAcadémie, la formation en ligne sur la sécurité informatique gratuite et ouverte à tous https://www.secnumacademie.gouv.fr/
- SecNumedu, labellisation de formations initiales en cybersécurité de l'enseignement supérieur https://www.ssi.gouv.fr/entreprise/formations/secnumedu/
- SecNumedu-FC, labellisation de formations continue en cybersécurité https://www.ssi.gouv.fr/entreprise/formations/secnumedu-fc-labellisation-de-formations-continues-en-cybersecurite/
- Kaspersky Lab propose une plate-forme de formation En Ligne dédiée aux employés, conçue pour enseigner et consolider les compétences techniques en matière de cybersécurité. Présentée sous forme d'outil interactif à l'accès modulaire, elle est recommandée pour former efficacement à la sécurité tous les employés non-spécialistes en informatique https://www.kaspersky.fr/enterprise-security/security-awareness

AUTRES ACTIONS DE SENSIBILISATION

- « *L'abandon* » d'une clef USB dans un endroit visible de l'organisation, avec un logiciel de cryptage installé dessus (voir Scénario d'incident 1 : clef page 126)
- De faux appels, pour l'arnaque aux présidents,
- Les intrusions physiques dans les locaux par des personnes étrangères à l'organisation,
- L'accès à des locaux protégés par des personnes de l'extérieur,
- La tournée dans les bureaux, pour vérifier si les ordinateurs sont éteints ou attachés,
- La vérification des bureaux (politique du bureau vide),
- La vérification du circuit du recyclage des papiers (prestataire),
- Le Chiffrement des ordinateurs (voir Scénario d'incident 3 : ordinateur vole, perdu…page 129).

Annexe n°15 Questionnaire de l'interview de RSSI (Responsable de la Sécurité du système d'information)

VOUS

- Quel est notre parcours et comment êtes-vous venu à la sécurité informatique ?
- Avez-vous une formation spécifique ?
- Depuis combien de temps travaillez-vous dans le domaine de la sécurisation ?

PERIMETRE

- Quel est le secteur économique des entreprises avec lesquelles vous travaillez ? (Privé, publique, banque, retail)
- Quel est votre périmètre d'intervention ? (Audit, conseil, formation, technique)
- Méthode et approche
- Concernant la sensibilisation des acteurs de l'entreprise, appliquez-vous une méthode éprouvée ou vous adaptez-vous à la situation du moment ? Ou un mixte ?
- À votre avis, qu'elle est la bonne approche ?
- Votre approche est-elle identique quelle que soit la population ou différente ?
- Quelle approche fonctionne et avec quel type de population ?
- Utilisez-vous des approches « cognitives » ou de « manipulation » pour imprimer les messages et engager les utilisateurs (exemple du livre : « Petit traité de manipulation pour les gens honnêtes »)

SENSIBILISATION

- Comment inciter les acteurs de l'entreprise à suivre une formation à la sensibilisation (sous quelque forme que ce soit) ?
- Comment mesurez-vous que la sensibilisation a porté ses fruits ?

SUPPORT

À votre avis, quel est le meilleur support de diffusion de message et pourquoi Gadgets (post-it, clef sécurisée, calendrier).

- Fond d'écran
- Clip vidéo
- Plaquettes, prospectus, support écrit
- Affiches
- Clef USB « pirate »
- Bande dessinée
- L'Intranet (diffusion d'informations d'actualité, des guides de bonnes pratiques, des contacts, des alertes sur les menaces).
- Un bulletin d'information sécurité adressée aux utilisateurs / à la direction / un blog ?
- Des courriels ciblés ou ponctuels suivant l'actualité
- Des campagnes de courriels de type phishing pour tester la réaction des utilisateurs
- Des rendez-vous en face-à-face
- Intervention dans les réunions (CODIR, réunion de cadres, réunion avec les syndicats, réunion hebdomadaire d'équipe etc.)
- Formation des utilisateurs en présentiel par vous-même ou un intervenant extérieur
- Formation en formation en ligne
- Produire de la documentation (la documentation utilisateur qui accompagne les logiciels… Mentionne les risques principaux encourus vis-à-vis de la protection des informations, les points de vigilance pour l'utilisateur et les recommandations types à mettre en œuvre).
- Des Serious Game adaptés au secteur d'activité / des Serious Game génériques
- Un module sécurité est inclus dans le séminaire d'entrée

IDENTITE

Pensez-vous que le service sécurité doit avoir « son » identité (comme Attitude3D à la SNCF) ?
Utilisez-vous les codes couleur dans les documents, support…

- https://www.celinedesign.com/blog/mettez-de-la-couleur-dans-vos-creations.php
- http://evolutiongraphique.com/la-signification-cachee-des-couleurs-en-communication-visuelle/

PROJET

Dans le cadre des projets pensez-vous qu'il faille intervenir :

- En amont du projet,
- Pas du tout,
- Pendant le projet,
- A posteriori

Avez-vous établi un document de type pour analyser les risques dans les projets de type Qersi-S (https://www.sante-centre.fr/portail/services/effi-centre-catalogue-de-services/effi-ssi,237,382.html)

ECONOMIE

Avez-vous réalisé une étude de coût concernant la non-sécurisation des informations ?
Avez-vous réalisé une étude de coûts des différentes approches (prix de gadgets, affiches) ? Dans l'affirmative quel est l'ordre d'idée ?
Qu'elle est la part du budget, en moyenne, consacrée à la sensibilisation des utilisateurs dans une entreprise ou par secteur économique ?

AUTRES COMMENTAIRES (LIBRE)

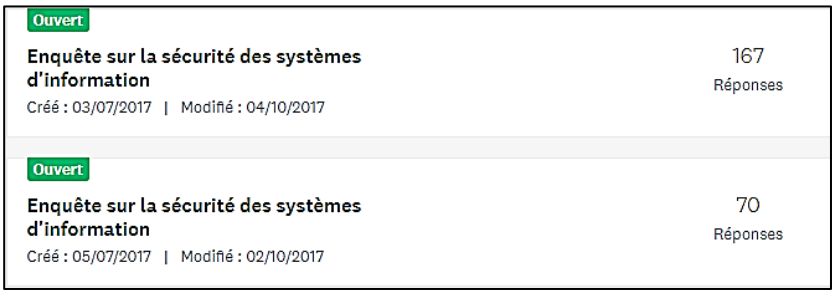
Annexe n°16 Liste des risques relevés lors du patient traceur

UN ORDONNANCEMENT, PAR LA FREQUENCE DES RISQUES,

	ÉTABLISSEMENTS										
TYPE DE RISQUE	A	B	C	D	E	F	G	H	Total	**Nombre de risques**	**Nombre de risques / par nombre de sites (8)**
La gestion des droits et profils : gérer l'accès à l'information	1	1		2		3	2	2	11	6	75,00 %
La dégradation de l'information et gestion : perte ou altération d'information, contamination par des virus et gestion d'incidents en cas d'incident majeur			5	2		5	3	3	18	5	62,50 %
Sensibilisation des agents à la protection de l'information.		1		3		2		2	8	4	50,00 %
TOTAUX	**1**	**2**	**5**	**7**	**0**	**10**	**5**	**7**	**37**	**15**	

ID n° 100 ordonnancement, par la fréquence des risques

Annexe n°17 Nombre de répondants à l'enquête sur la plateforme SurveyMonkey



Annexe n°18 Résultats de l'enquête des professionnels de la sécurité

REPARTITION DES REPONDANTS (LES CINQ PREMIERS)

TYPE	NOMBRE DE PARTICIPANT
RSSI	75,61 %
RSI	6,50 %
DSI	5,69 %
RSSI + CIL	4,07 %
Directeur projet/Chef de projet	4,07 %
DSSI	4,07 %
Total général	100,00 %

ID n° 101 Fonction des répondants

REPARTITION DES RSSI EN SECTEUR PRIVE OU PUBLIC

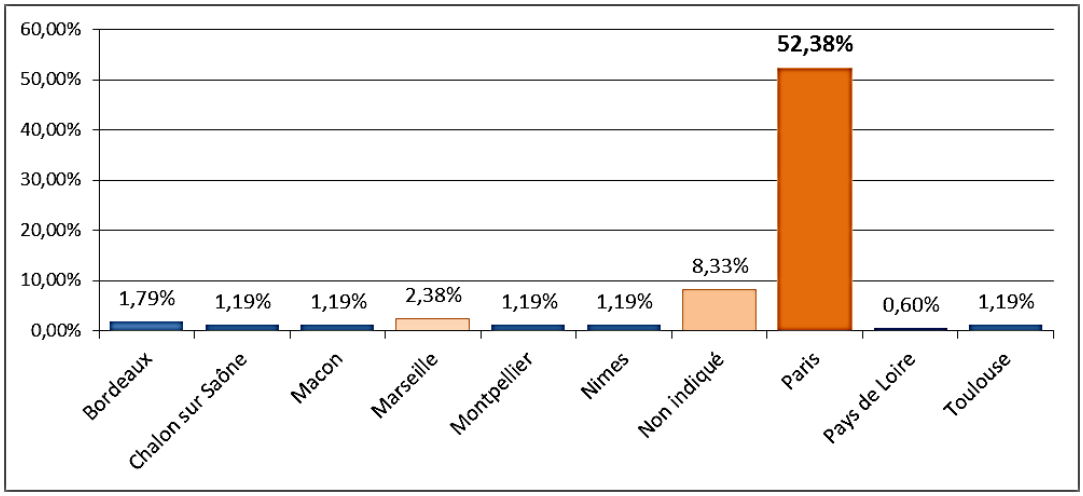
- Privé ..... 37,50 %
- Publique ..... 62,50 %

SECTEUR D'ACTIVITE DES RSSI

ÉTIQUETTES DE LIGNES	NOMBRE DE PARTICIPANT
Santé	37,18 %
Non indiqué	19,23 %
Finance	19,23 %
Conseil - Service	12,82 %
Industrie	11,54 %

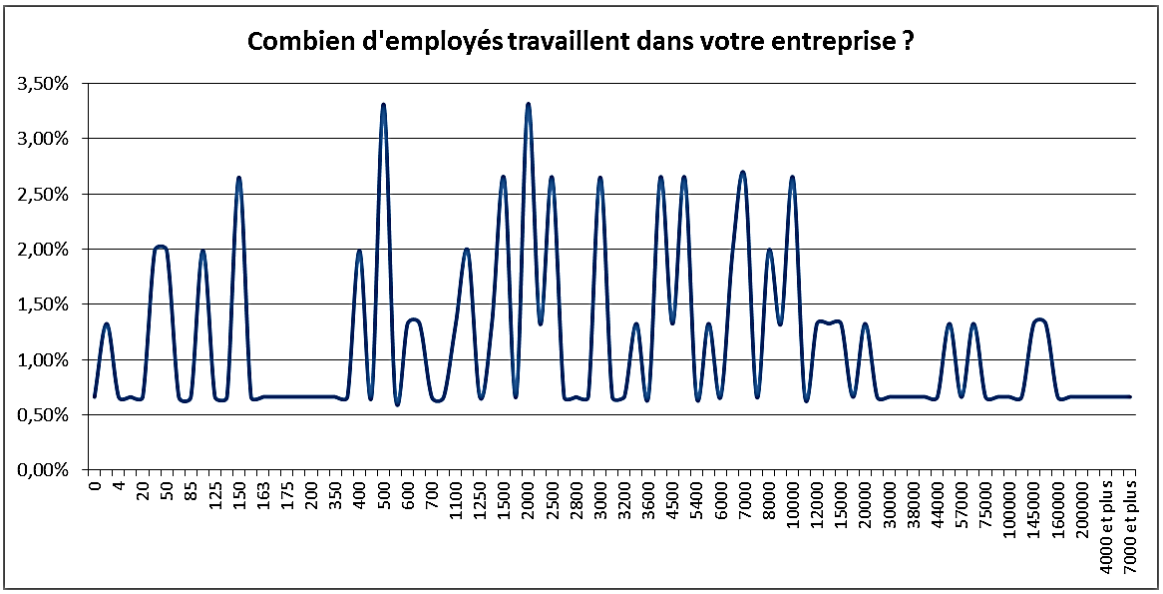
ID n° 102 Quel est le secteur d'activité des répondants

IMPLANTATION DES ORGANISATIONS REPONDANTES



ID n° 103 Implantation des organisations répondantes

TAILLE DES ORGANISATIONS QUI ONT REPONDU



ID n° 104 Taille des organisations qui ont répondu

CE QUI EST A PROTEGER

CE QUI EST A PROTEGER	REPONSES EN %
Vous traitez des données sensibles (données personnelles, données personnelles de santé, données classées défense)	83 %
Vous avez défini et formalisé par écrit les objectifs de sécurité informatique pour votre établissement	76 %
Vous avez communiqué à votre Direction	82 %
Vous avez déterminé vos vulnérabilités informatiques et évalué les pertes financières (directes ou indirectes) qu'elles pourraient occasionner.	55 %
Vous connaissez-vous votre "risque maximal tolérable" (RMT)	75 %
En cas d'indisponibilité durable de votre système informatique, par exemple aujourd'hui, savez-vous dans quel délai vos services pourraient reprendre une activité normale.	69 %
Autre remarque, observation ?	12 %

ID n° 105 ce qui est à protéger

METHODES EMPLOYEES POUR L'ANALYSE DE RISQUE (CINQ PREMIERS)

METHODES	NOMBRE DE PARTICIPANT
Non répondu	51,25 %
Ebios	38,13 %
Mehari	4,38 %
Méthodologie interne	3,75 %
Dérivée de Ebios	2,50 %
Total général	**100,00 %**

ID n° 106 Méthodes employées pour l'analyse de risque

SENSIBILISATION DES PRESTATAIRES/PARTENAIRES

- OUI.....74
- NON 95

INTERVENEZ-VOUS DANS LA SECURITE DES PROJETS ?

En amont du projet	71 %

Pas du tout	3 %
Pendant le projet	65 %
A posteriori	43 %
Avez-vous établi un document type pour analyser les risques dans les projets de type Qercy (https://www.sante-centre.fr/portail/services/effi-centre-catalogue-de-services/effi-ssi,237,382.html)	34 %

ID n° 107 intervenez-vous dans la sécurité des projets ?

SUR QUELLE NORME VOTRE SMSI (SYSTEME DE MANAGEMENT DE LA SECURITE DE L'INFORMATION) EST-ELLE BASEE ?

SMSI	NOMBRE DE PARTICIPANT
ISO 27xxx	55,03 %
Non répondu	44,38 %
COBIT	0,59 %

ID n° 108 Sur quelle norme votre SMSI (système de management de la sécurité de l'information est-elle basée

Vous avez établi des chartes à l'usage des utilisateurs/administrateurs/personnels IT, annexées au contrat de travail ou aux règlements intérieurs.	82 %
Ces chartes sont obligatoires	67 %
Vous avez homologué votre SI ou certaines parties (homologation de type ANSSI https://www.ssi.gouv.fr/guide/lhomologation-de-securite-en-neuf-etapes-simples/)	27 %
Vous avez un budget consacré à la sécurité	54 %

ID n° 109 Sur quelle norme votre SMSI (système de management de la sécurité de l'information est-elle basée

CONNAISSANCE DU RGPD DANS LES ORGANISATIONS

	OUI	NON
Non indiqué	5	8
Secteur Privé	79	17
Secteur public	48	12
Total général	**132**	**37**

ID n° 110 Connaissance du RGPD dans les organisations

% DE PREPARATION	PRIVE %	PUBLIQUE %
0	31 %	25 %
25	25 %	38 %
50	25 %	17 %
75	14 %	7 %

ID n° 111 Répartition du taux de préparation

SUPPORTS DE SENSIBILISATION UTILISES DANS LE PRIVE ET LE PUBLIQUE

TYPE DE SUPPORT	MOYENNE
Mails ciblés	79 %
Intranet	73 %
Réunions	69 %
Formation des utilisateurs en présentiel	56 %
Documentation	43 %
Séminaire d'entrée	39 %
Campagnes d'courriels phishing	38 %
Rendez-vous en face-à-face	31 %
Bulletin d'information sécurité	28 %
Formation en ligne	28 %
Serious Game génériques	12 %
Serious Game adaptés	10 %

ID n° 112 Supports de sensibilisation utilisés dans le privé et le publique

ÉTIQUETTES DE LIGNES	BULLETIN D'INFORMATION	INTRANET	COURRIELS CIBLES	CAMPAGNES D'COURRIELS	RENDEZ-VOUS EN FACE-A-FACE	REUNIONS	FORMATION DES UTILISATEURS EN	FORMATION EN LIGNE	DOCUMENTATION	SERIOUS GAME ADAPTES	SERIOUS GAME GENERIQUES	SEMINAIRE D'ENTREE
Administration		■	■	■			■			■		■
Administration - Défense	■	■	■	■	■	■	■			■		■
Administration - Finance	■	■	■		■	■	■	■	■			■
Administration - Justice						■	■					
Administration - Sécurité Intérieure			■			■			■			
Administration - Social	■	■	■		■	■	■					
Assurance	■	■	■	■	■	■	■	■	■		■	■
Automobile		■	■			■						
Bancaire	■	■	■	■	■	■	■	■	■	■	■	■
Bancaire - Assurance	■	■	■	■		■	■	■	■	■		■
BTP	■	■	■	■	■	■	■	■	■			■
Collectivité locale		■	■			■	■		■			■
Collectivité territoriale	■	■	■	■	■	■	■	■	■	■	■	
Commerce de gros		■	■	■	■	■	■	■	■	■		■
Conseil - Service	■	■	■	■	■	■	■	■	■		■	
Culture			■		■	■						
Distribution	■	■	■	■	■	■	■	■	■	■		■
Editeur de logiciels		■	■		■	■	■		■			
Emploi		■	■		■	■	■		■			■
Energie		■	■		■	■	■		■		■	■
Finance	■	■	■	■	■	■	■	■	■	■	■	■
Hôtellerie - Restauration	■		■	■	■	■	■					■
Immobilier	■	■	■		■		■	■	■			
Industrie	■	■	■	■	■	■	■	■	■	■	■	■
Industrie - aéronautique		■	■		■			■	■			
Industrie composants électriques/électroniques		■	■			■		■				
Informatique	■	■	■	■	■	■	■		■			■
Luxe	■	■	■	■	■	■	■	■	■			■
Manufacturing			■			■						
Médias		■	■	■		■					■	■
Mutuelle	■	■				■		■			■	
Non indiqué	■	■	■	■	■	■	■	■	■	■	■	■
Recherche			■			■	■		■			
Sanitaire - médicaux social		■	■		■	■	■		■			
Santé	■	■	■	■	■	■	■	■	■	■		■
Sécurité privée	■	■	■			■	■					
Service numérique	■	■	■	■	■	■	■	■	■	■	■	■
Systèmes d'information information		■	■									
Télécommunications	■	■	■	■	■	■	■	■	■		■	■
Tourisme fluviale							■					
Transport	■	■	■	■	■	■	■	■	■	■	■	■

ID n° 113 Support de communication par secteur d'activité

SELON VOUS, QU'ELLE EST LA OU LES METHODES DE SENSIBILISATION LES PLUS EFFICACES ? ET POURQUOI ?

QUEL EST LE SECTEUR D'ACTIVITE DE VOTRE ENTREPRISE ?	QUELLE EST VOTRE FONCTION ?	SELON VOUS, QU'ELLE EST LA OU LES METHODES DE SENSIBILISATION LES PLUS EFFICACES ? ET POURQUOI ?
Administration	RSSI	Le présentiel de loin car on peut apprécier les comportements suite à des situations réelles venant de l'entreprise.
Administration - Défense	RSSI	Séances de sensibilisation obligatoire en amphi
		Vivre un incident en direct… Mais coûteux… ;)
Administration Finance	DSSI	Le présentiel mais ça n'est pas toujours possible
Administration - Justice	RSSI	Formations et serious games, mais selon moi l'efficacité des différentes méthodes dépend de la culture d'entreprise. Selon les cas d'autres méthodes peuvent être très efficaces (films, formation en ligne)
Administration - Sécurité Intérieure	RSSI + CIL	Le debriefing après une alerte virale détectée. Après une petite chaleur, l'utilisateur est plutôt réceptif…
Administration - Social	Fonctionnaire de Sécurité des Système d'Information	Le face-à-face avec les métiers
Assurance	RSSI	Formation en ligne
		Formation en présentiel avec un format court, ciblé sur un ou deux sujets maximums, assuré par l'équipe SSI interne Les formations en présentiel permettent de personnifier l'équipe SSI et de renforcer sa visibilité dans l'entreprise, et de faire passer les messages plus efficacement. E-learning/serious game en plusieurs modules courts répartis tout au long de l'année Les modules en ligne réparties dans le temps permettent d'assurer une sensibilisation continue. Courriel ou message sur l'intranet en cas de menaces imminentes ou d'incidents, rappelant les bons réflexes à adopter, l'impact de l'incident. Ces courriels/messages marquent les esprits et permettent une réaction rapide des utilisateurs.
		La combinaison de plusieurs approches et supports
		Pas une, mais un ensemble. Important de changer de méthode régulièrement
		Toute action de sensibilisation est efficace si elle réussit à toucher le public concerné. C'est-à-dire qu'il y a un véritable travail en amont de réflexion. La sensibilisation est à adapter en fonction de l'auditoire. Ce qui marche bien : - la répétition (formation en ligne annuelle, type bourrage de crâne à partir de situations réelles d'entreprise) - animer la sensibilisation : donner des cadeaux, organiser des concours avec "podium" pour les meilleurs (ce que je fais). - Utiliser l'humour, les animations (j'ai eu beaucoup de retours positifs suite à mon dernier courriel que je peux communiquer) - utiliser les vidéos (excellentes vidéos sur le Net) qui illustrent des cas réels - utiliser ce qui arrive réellement en entreprise : exemple de message reçu, conséquences du clic… etc. - utiliser des accroches chocs (par exemple dans l'objet des courriels envoyés). - Intervenir le plus possible pour donner de la visibilité au RSSI, cela engendre de la sollicitation…
	RSSI adjoint	Je pense que la sensibilisation en face-à-face est la meilleure. Elle permet d'expliquer, d'imager et de transposer les risques dans le contexte pro et privé du collaborateur. Elle est adaptative.
		Les messages liés à l'actualité qui permettent de lier les risques potentiels aux évènements réels.

QUEL EST LE SECTEUR D'ACTIVITE DE VOTRE ENTREPRISE ?	QUELLE EST VOTRE FONCTION ?	SELON VOUS, QU'ELLE EST LA OU LES METHODES DE SENSIBILISATION LES PLUS EFFICACES ? ET POURQUOI ?
Automobile	DRH	La multiplication des informations utilisant plusieurs canaux ou supports.
	RSSI	Nous avons opté pour un outil de sensibilisation et protection contre les risques internes qui nous aide sur la GDPR, les comportements à risques etc. C'est automatisé couvre les utilisateurs, les techniques et il suffit de rajouter une règle si l'on veut renforcer une surveillance. Nous avons des alertes et des vidéos pouvant faire preuve du comportement malveillant (vol de donnes, tentative d'extraction etc.…) nous avons mis en place cet outil suite à des soupçons de communication externe de données.
Bancaire - Assurance	Directeur projet/Chef de projet	Il n'y a pas de méthode meilleure que les autres, il faut toutes les combiner.
	Responsable Gouvernance IT et Sécurité IT	Présentiel
	RSSI	Le cocktail de l'ensemble. L'efficacité tient à la répétition, mais si elle n'est faite que d'une seule manière, c'est la lassitude qui l'emporte. Donc un discours cohérent porté de multiples manières.
		La formation en ligne est en cours de mise en place ainsi que des campagnes et démonstrations piratage/phishing.
		Serious game
		Toutes les méthodes sont bonnes… Chaque personne réagit en fonction de sa sensibilité. Il est donc essentiel de multiplier les canaux de communication et de répéter régulièrement les messages. Aujourd'hui on constate que les gens savent et connaissent les consignes, mais ils ne les respectent pas.
		Toutes, elles doivent être combinées
	RSSI + CIL	Celle qui marque et passe peu de messages. La méthode dépend du public
BTP	DSSI	Rendez-vous face à face, car ciblé et interactif. Campagne type phishing : car proche du réel c'est la sensibilisation qui utilise aussi bien le domaine personnel que professionnel pour que les personnes se sentent concernées personnellement, le média le plus efficace est le présentiel
	RSSI	La meilleure sensibilisation est la personne qui elle-même passe des messages importants à ses collègues.
Collectivité locale	DSI adjoint + RSSI	Je ne pense pas qu'il y ait une bonne méthode car : 1) les gens oublient et 2) les sensibilités de chacun sont différentes. À mon sens, il faut donc : 1) de la fréquence et 2) de la diversité dans la sensibilisation.
	RSSI	La méthode la plus efficace me paraît la méthode en face-à-face. Elle permet de faire passer des messages personnalisés en travaillant sur les résistances.
Collectivité territoriale	RSSI	Formation en présentiel car appréhension de cas concrets et vécus
	RSSI + CIL	Face à face
		Présentiel auprès d'un groupe d'utilisateurs en partant de fait quotidien. C'est plus parlant pour l'utilisateur et cela l'intéresse.
		Toutes les méthodes sont utiles et efficaces car chaque utilisateur va être sensible à une ou plusieurs de ces formes mais jamais tous avec la même. En présentiel j'utilise également les ressources de type serious-games que l'on retrouve en

QUEL EST LE SECTEUR D'ACTIVITE DE VOTRE ENTREPRISE ?	QUELLE EST VOTRE FONCTION ?	SELON VOUS, QU'ELLE EST LA OU LES METHODES DE SENSIBILISATION LES PLUS EFFICACES ? ET POURQUOI ?
		formation en ligne. Les serious games marchent très bien pour modifier les comportements mais doivent être reliés aux autres modes de communication : informations régulières dans le journal interne, sur l'intranet,… et chaque fois que nécessaire en fonction de l'actualité
Commerce de gros	Directeur des risques	C'est la combinaison des méthodes avec répétition des messages sous des formes différentes qui permet des résultats. Courriels tests de phishing, serious games et E-learning.
	DSSI	Courts ateliers pratiques en présentiel pour construire un contact humain et une relation de confiance.
	RSSI	Définition d'un plan global utilisant différents médias, et adaptant le contenu des messages aux cibles.
Conseil - Service	Chargée de communication cybersécurité	En présentiel afin de montrer réellement les risques. Les courriels sont plutôt noyés dans la masse.
	Consultant sécurité information	Il est important d'adopter plusieurs vecteurs de sensibilisation car chaque personne sera sensible a des vecteurs différents (gamification ; challenge ; immersion ; démonstration ; informations…)
	DP	C'est notre ADN
	DPO	J'ai mis en place des sensibilisations/formations pour des personnes clefs de l'entreprise essentiellement dans des fonctions supports (à l'informatique, au juridique, à la RH, aux achats, à la finance…) J'ai également fait du théâtre d'entreprise avec des pièces jouées par de vrais acteurs et un scénario adapté au secteur d'activité (http://www.guichets-fermes.com/ pour ne pas les citer). Ces saynètes ont été filmées et diffusées sur l'intranet. Les images et l'aspect ludique de cette méthode marquent les esprits.
	DSI	La redondance : plusieurs supports répétés dans le temps.
	Formateur conseil	Je ne sais pas
	RSSI	Présentation des grandes menaces et interactions avec les participants. (Lien à faire avec la vie personnelle). Sensibilisation via des vidéos (analogie risque informatique et voiture) a également bien fonctionné.
Culture	RSI	Étude de cas concrète et proximité
Distribution	RSSI	Des méthodes, une seule méthode n'est pas suffisante. Il faut diffuser la sécurité dans l'entreprise en s'adaptant aux interlocuteurs
		Même si l'audience est plus faible (qu'un envoie en masse de courriel), le meilleur impact est obtenu par les animations faites sur site. Nous avons développé un jeu d'évasion grandeur nature (escape game) basé sur la SSI (première en France à ma connaissance), il a eu un succès phénoménal mais vu la taille de l'entreprise, peu de gens l'ont suivi.
Editeur de logiciels	RSSI	Base d'information sur wiki [318]Confluence. Petite structure d'ingénieurs tous dans la sécurité. On responsabilise en réponse aux incidents et par des exemples. Nous avons plusieurs réseaux totalement séparés et tout le monde sait que l'on ne passe pas de l'un à l'autre. Espaces différents avec portes fortes, badges et lecteurs

[318] Un wiki est une application web qui permet la création, la modification et l'illustration collaboratives de pages à l'intérieur d'un site web. Source wikipédia

QUEL EST LE SECTEUR D'ACTIVITE DE VOTRE ENTREPRISE ?	QUELLE EST VOTRE FONCTION ?	SELON VOUS, QU'ELLE EST LA OU LES METHODES DE SENSIBILISATION LES PLUS EFFICACES ? ET POURQUOI ?
		biométriques, plus vidéosurveillance. Cela fait plus que sensibiliser. Un datacenter dans un bunker.
Emploi	DA innovation et RSE	Il est important de multiplier les canaux pour toucher et sensibiliser au maximum
Energie	RSSI	Cas concret
		Des rendez-vous en face-à-face
		Une méthodologie sur l'année, en continu. Il faut mieux un peu toute l'année, qu'une grosse sensibilisation 1 fois / an donner des exemples concrets, qui parlent aux gens et qui les marquent. Les faire parler, échanger entre eux
		Visite de terrain
Finance	Maîtrise d'Ouvrage Stratégique Sécurité Groupe	Test phishing, formation en ligne jeu avec un lot gagnant autour de la connaissance du phishing, et autres fraudes.
	RSSI	Campagne de phishing factice
		Changer régulièrement pour éviter les habitudes. Prospectus, courriels, affichettes coin café, intervention DGSI, etc.
		Face à face, et en racontant une histoire, et faire réagir
		Il n'y a pas de méthodes plus efficaces que d'autres : Il faut que ce soit multicanal car chaque personne est sensible aux informations de façon différentes. Chez nous, nous passons par : - Formation en ligne annuelle - Affiches dans les salles de pause - Diffusion d'article sur l'actualité dans la gazette (diffusion trimestrielle) - Démonstration de piratage informatique en live Je souhaite mettre en place des BD dans les couloirs et post-it.
		Intervention en "amphi" avec exemple d'incidents externe et interne
		La simulation (envoi de faux courriels, faux appels téléphoniques, réaliser de fausses intrusions logiques et physiques) reste le moyen le plus marquant et le plus efficace en termes de sensibilisation à la SSI.
		Le face-à-face et la formation en présentiel, car on adapte son discours à la réaction de la personne en face de soi.
		Pas de "la plus efficace" ! Il faut un peu de tout pour garder une dynamique constante.
		Plusieurs méthodes combines, une seule n'est pas efficace. Il faut surprendre et innover vis-à-vis de la DG et des utilisateurs
		Site intranet, module SSI à l'accueil des nouveaux arrivants et courriels trimestriels avec liens sur les documents "chartes" et "PCA".
	RSSI + DPO	La meilleure est, je pense, une concaténation de ces différentes pratiques !
Hôtellerie - Restauration	Cuisinier	Information des risques. Obligation de faire figurer dans le règlement intérieur les obligations de sécurité et les PUNITIONS en cas de non-respect de celle-ci (par exemple des fessées publiques donner par le directeur informatique).
	RSSI	Les séances de formations en s'appuyant sur des cas concrets et en sortant du monde professionnel.
Immobilier	RSSI	Les campagnes de phishing car elles permettent une sensibilisation active de l'utilisateur (apprendre par l'erreur). Prévu à court terme au sein de mon organisation
		News en lien avec l'actualité et Réunion de sensibilisation aux équipes

QUEL EST LE SECTEUR D'ACTIVITE DE VOTRE ENTREPRISE ?	QUELLE EST VOTRE FONCTION ?	SELON VOUS, QU'ELLE EST LA OU LES METHODES DE SENSIBILISATION LES PLUS EFFICACES ? ET POURQUOI ?
Industrie	DSSI	Les interventions, séminaires d'entrée et communication courriels
	RSI	Je ne sais pas
	RSSI	Formation en ligne semestrielle obligatoire. S'il ne le suit pas, l'utilisateur perd l'accès à divers services informatiques dont l'accès à Internet.
		Il n'y a pas de méthode unique, la réponse dépend des profils métier et d'âge.
		Les réunions d'information en petit groupe (12 personnes max.) ou les entretiens en tête à tête, en clair lorsqu'il y a un contact humain direct avec le RSSI.
		Phishing
		Sensibilisation par manager à la prise de fonction
		Une approche multiméthode est nécessaire, car chacune a ses forces et faiblesses. Une action présentielle est plus frappante, mais touche un public réduit. Une approche médiatique (courriel, intranet) touche plus de monde, mais ne permet pas de répondre aux questions et de clarifier les actions à suivre.
Industrie - aéronautique	Responsable sécurité infogérant	Séminaire parce que les formations en lignes sont trop récentes pour être qualifiées.
Industrie composants électriques/électroniques	RSSI	Face à face, les autres ne permettant que rarement l'implication réelle des participants et la compréhension de leur rôle de la défense de notre SI.
Informatique	Consultant sécurité information	Charte informatique et réunions d'information /publipostage afin de démystifier la sécurité et démontrer la valeur en termes de protection du salarié puis de la société.
		Réunion / courriels / démonstrations / intervention Codir adaptés à la population l'actualité un projet spécifique La formation en ligne n'a pas d'intérêt sauf à pouvoir y consacrer des finances importantes pour personnaliser les supports les entretenir et les faire évoluer dans le temps Une expérience de plus de 15 ans
Luxe	RSSI	Aucune plus efficace il faut multiplier les approches
		Phishing campagne et présentiel
		Une sensibilisation soutenue et des réunions en petits comités pour recevoir les cas d'usage qui sont ceux qui posent problème.
Manufacturing	DSI	Serious game, la sensibilisation doit être ludique
Médias	DSI adjoint + RSSI	Les fausses campagnes et le serious game avec des choses à gagner à condition de tout faire et de finir à 100 % de réussite.
Mutuelle	RSSI	Réunion publique sur la sécurité
Non indiqué	RSSI	Communication régulière, courriel sur l'actualité
		Mise en place d'une phase d'observation dans la vie de tous les jours. La période est indiquée sur 1 mois, mais le jour, et l'heure non précisés. Derrière une restitution immédiate l'enregistrement n'étant pas possible. Le face-à-face, ou serious game sur un délai d'observation avec mise en situation dans la vie de tous les jours. Permet une analyse du comportement en temps réel, et une correction à la personne
		Pas de méthode la meilleure dans l'absolue dépend du public (âge, métier, fonction,…) notamment multiples déclinaisons à trouver les formats courts semblent plus adaptés formats qui "implique" les personnes (VS passivité)
		Séance de sensibilisation
		Sensibilisation sous forme de formation en physique basé sur des cas concrets

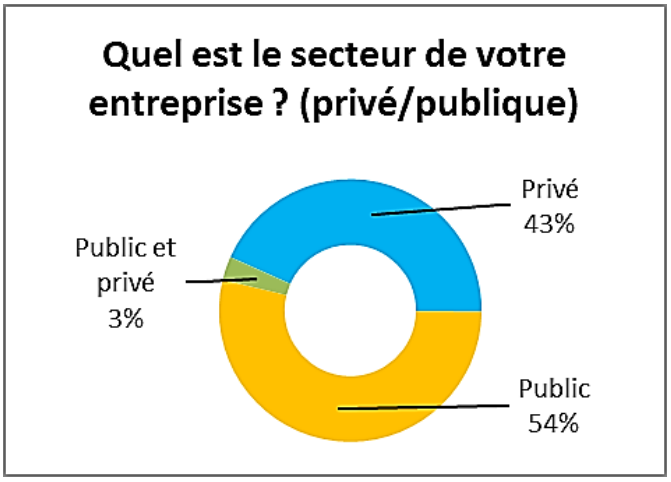
QUEL EST LE SECTEUR D'ACTIVITE DE VOTRE ENTREPRISE ?	QUELLE EST VOTRE FONCTION ?	SELON VOUS, QU'ELLE EST LA OU LES METHODES DE SENSIBILISATION LES PLUS EFFICACES ? ET POURQUOI ?
		Tests et courriels provenant de la direction
		Tous azimuts.
Recherche	RSSI	Communication de la direction. Contact direct avec les divers acteurs
Sanitaire - médicaux sociaux	RSI	Procédure visuelle
		Rappeler les principes de sécurité en permanence et par tous les moyens !
	RSI + Qualité	Rendez-vous en face-à-face
	RSI + RSSI	Des mises en situation réelle, faux courriel ouvrant une fenêtre indiquant à l'utilisateur que PC vient d'être piraté par exemple…
Santé	Administrateur réseaux & systèmes	Un cas concret ou les utilisateurs se retrouvent vraiment plantés sinon ils considèrent que ça n'est pas leur problème.
	DAFSI	Rappels permanents directs (courriels) cause turnover et oubli des consignes…
	DSI	Des rendez-vous en face-à-face, permettant d'avoir une sensibilisation plus efficiente. Mais difficile à mettre en œuvre
		La méthode la plus efficace est malheureusement le retour d'expérience suite à un incident, ainsi les utilisateurs ont une vue concrète de ce qui peut se passer.
		Rendez-vous face à face, la pédagogie est l'art de la répétition…
		Une formation annuelle obligatoire sera mise en place en 2018 + communication (s) par le journal interne.
	DSI + RSSI	Le présentiel et des cas concrets
	DSIO	Le séminaire et les courriels d'actualité
		Courriels et séminaire d'entrée
		Sans doute le serious game, à l'embauche et rappels réguliers, afin que les personnels touchent du doigt la réalité des risques et de leurs conséquences.
		Un peu tout ça ;-)
	DSIT	Serious game
		Une combinaison de toutes et la nomination d'un RSSI pour répéter et répéter
	Référent SSI	Le contact humain et une explication face à face restent le plus efficaces selon moi. Une session de sensibilisation est un moment dédié où les utilisateurs se consacrent uniquement au sujet, contrairement à la formation en ligne. Le dialogue, les échanges, permet vraiment d'approfondir.
	Responsable de l'activité Conseil	Pour les utilisateurs : sensibilisation régulière avec mise en situation
	RSI	Présentation de la charte et explication de texte
	RSI + RSSI	Des campagnes visuelles avec 1 action répétée tous les trimestres. Pour la simplicité et le message marquant.
		Interventions dans les instances.
	RSSI	La sécurité repose sur la responsabilité et l'engagement des agents. Il n'y a donc pas de meilleure méthode, il n'y a que des méthodes adaptées pour un public. Il faut donc faire un peu tout ce qui est listé et être capable d'impliquer les gens. Ce dernier point repose plus sur l'entregent que sur quoi que ce soit d'autre.
		Le présentiel avec un kit (film et présentation) qu'on laisse aux cadres pour qu'ils rejouent dans leur réunion.
		Les interventions dans les services sur un sujet précis. Permet d'échanger directement avec les utilisateurs, sur des scénarios de risques concrets, qui peuvent les toucher dans leur travail, et en faisant le parallèle avec les risques à la maison.

QUEL EST LE SECTEUR D'ACTIVITE DE VOTRE ENTREPRISE ?	QUELLE EST VOTRE FONCTION ?	SELON VOUS, QU'ELLE EST LA OU LES METHODES DE SENSIBILISATION LES PLUS EFFICACES ? ET POURQUOI ?
		Les rendez-vous face à face et le séminaire d'entrée
		Par l'exemple il faut marquer les esprits
		Pédagogie
		Sensibilisation en formation
		Test de phishing et serious game
Sécurité privée	RSSI	Le présentiel est très efficace mais très chronophage. La formation en ligne, les courriels et l'affichage permettent de rappeler les bonnes pratiques à moindre coût.
Service numérique	RSI	Réunion face à face et/ou exemples de cas concrets
	RSSI	C'est un ensemble. La présentation, sensibilisation, puis au quotidien. Le + efficace serait de mettre la personne dans une situation concrète, mais c'est + difficile
		Formation en ligne avec test et serious game adapté pour les jeunes
		La campagne de phishing est très concrète, parle à tout le monde. L'intérêt est de pouvoir la réaliser régulièrement pour mesurer la progression de la sensibilisation du personnel.
		Les tests car les résultats sont basés sur du réel observé et non sur du potentiel hypothétique.
	RSSI + DPO	Les sensibilisations adaptées juste après une vague d'attaques : cas concrets, là les utilisateurs comprennent et apprennent
Systèmes d'information information	Directeur projet/Chef de projet	Serious game pour leurs aspects ludo éducatif
Télécommunications	Responsable Cellule d'Investigation Forensic	Campagnes ponctuelles d'information par courriel, gros titre sur l'intranet, affichages ponctuels dans les lieux de vie.
	RSSI	La complémentarité de plusieurs méthodes pour aborder les sujets dans leur diversité grâce aux différents formats des supports. De plus, cela rend "ambiant" le thème sécurité dans le quotidien des acteurs.
		On ne fait pas tout partout. Par exemple le face-à-face est réservé à une population particulièrement sensible mais pas pour les 22 000 employés.
		Sessions en amphithéâtre devant tous les collaborateurs pour balayer largement + modules de formation dédiée orientés sur certains métiers.
Tourisme fluvial	Administrateur réseaux & systèmes	Aucune idée, une sensibilisation sous forme de formation les salariés se sentent concerné au début puis lâche l'affaire, en ce qui concerne mettre en place des documents/mail pour sensibiliser les gens ne les lisent même pas. Le réel problème est que, tant que ça ne les concerne pas directement il ne s'en préoccupe pas.
Transport	Adjoint Responsable d'exploitation	Il faut s'appuyer sur les événements d'actualité pour montrer la réalité du danger
	DSSI	Rebondir sur l'actualité des cyberattaques qui sont très médiatisées. La formation présentielle
	Responsable sensibilisation sécurité informatique	Les méthodes collégiales impliquant les salariés en équipe
	RSSI	Je la cherche encore
		La sensibilisation en "réaction" à un incident, mineur ou majeur
		Multi canal le plus efficient toutes en fonction de la population

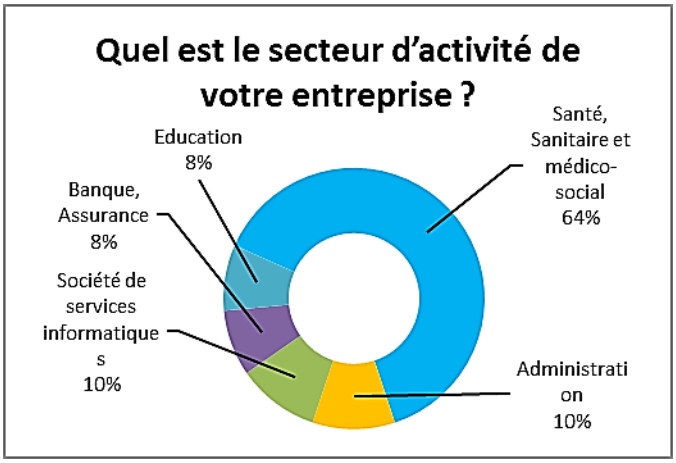
QUEL EST LE SECTEUR D'ACTIVITE DE VOTRE ENTREPRISE ?	QUELLE EST VOTRE FONCTION ?	SELON VOUS, QU'ELLE EST LA OU LES METHODES DE SENSIBILISATION LES PLUS EFFICACES ? ET POURQUOI ?
		(âge, culture, sensibilité aux différents canaux

ID n° 114 Selon vous, qu'elle est la méthode de sensibilisation la plus efficaces ? Et pourquoi

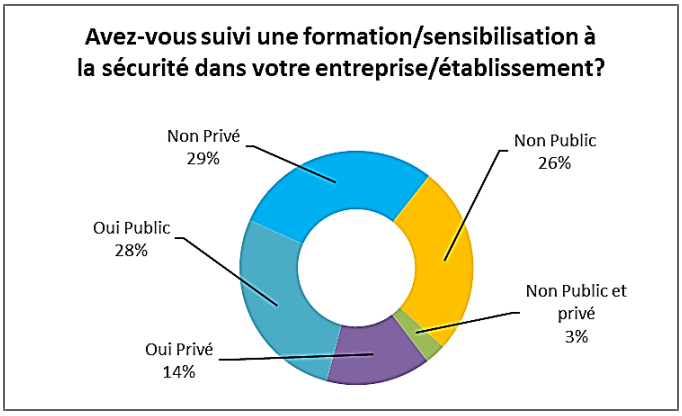
Annexe n°19 Résultats de l'enquête des non professionnels de la sécurité



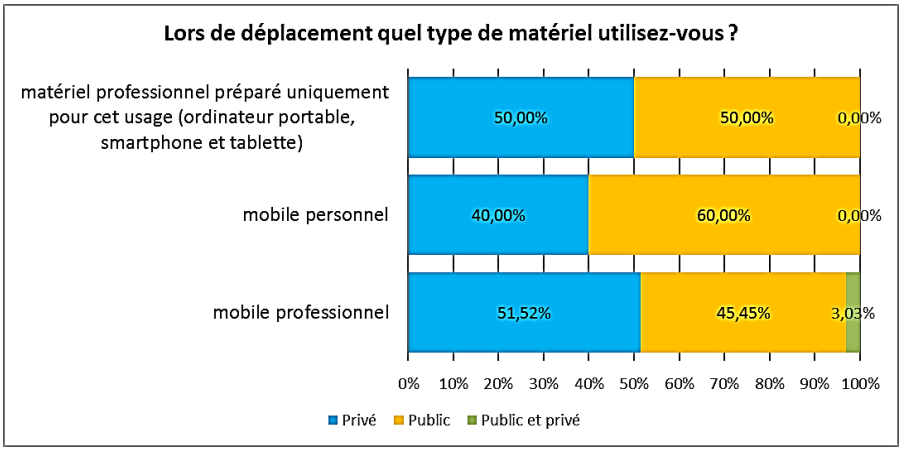
ID n° 115 Quel est le secteur de votre entreprise ?



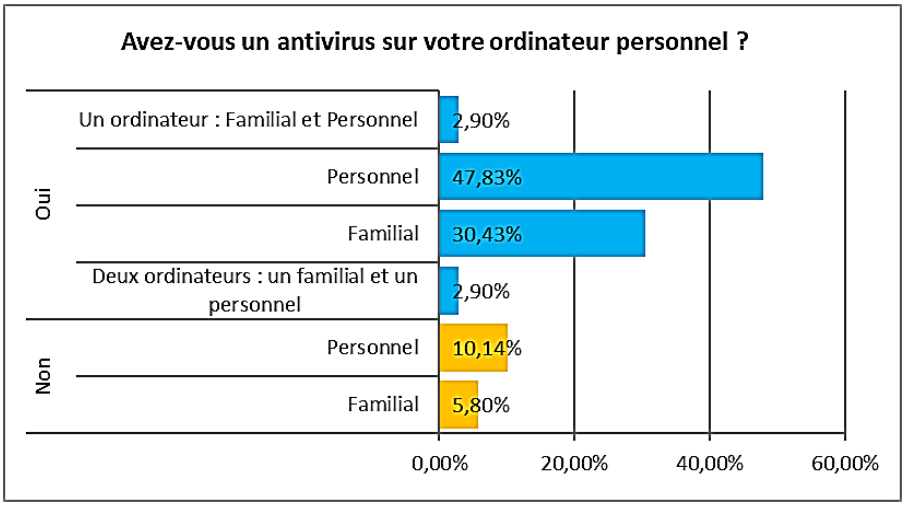
ID n° 116 Quel est le secteur d'activité de votre entreprise ? (5 premiers)



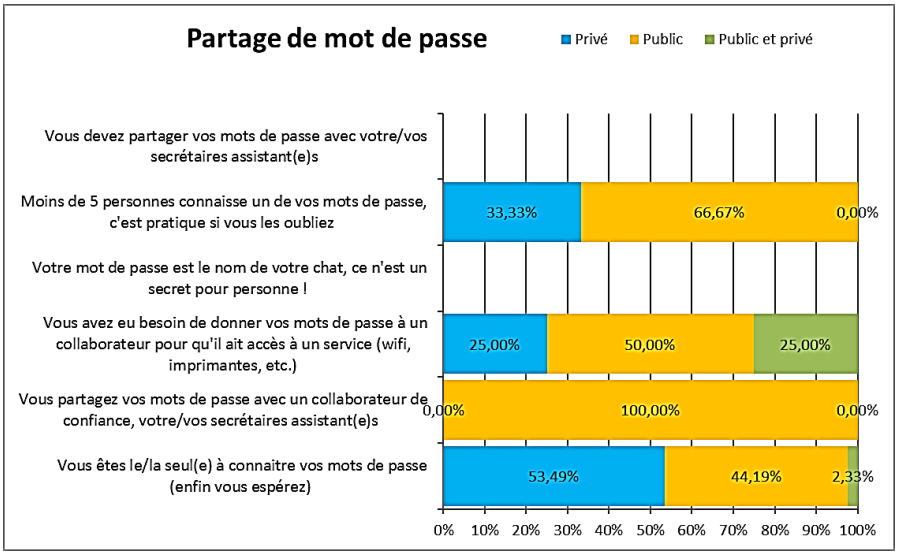
ID n° 117 Avez-vous suivi une formation/sensibilisation à la sécurité dans votre entreprise/établissement ?



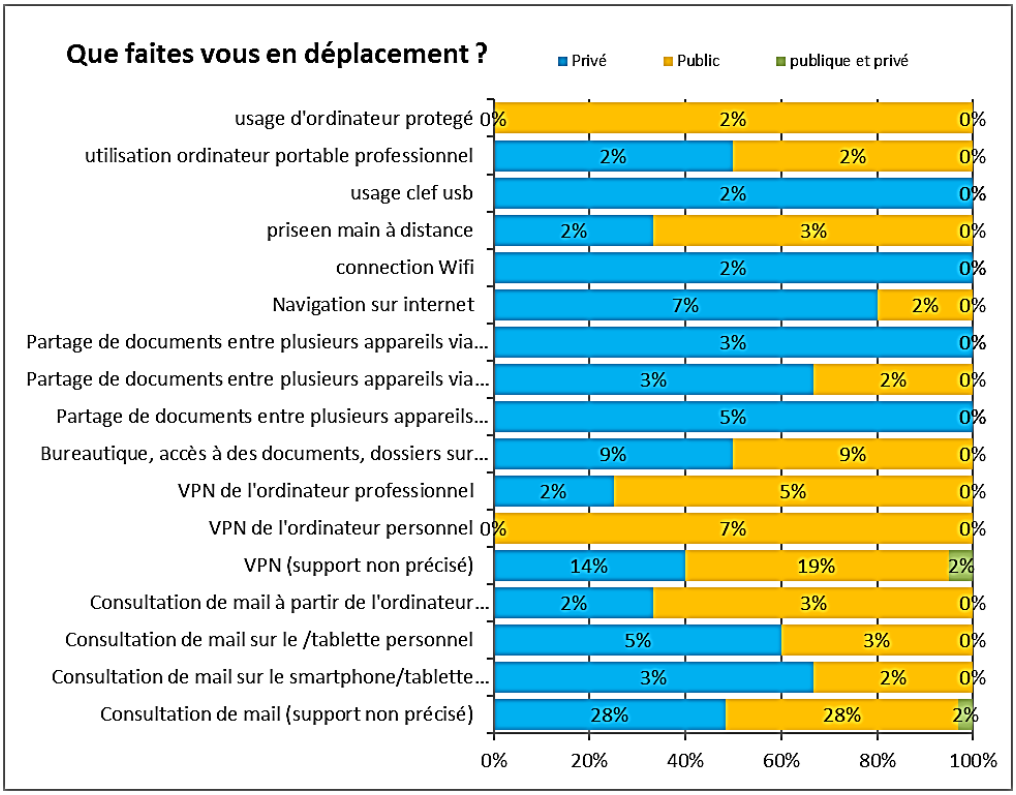
ID n° 118 Lors de déplacement quel type de matériel utilisez-vous ?



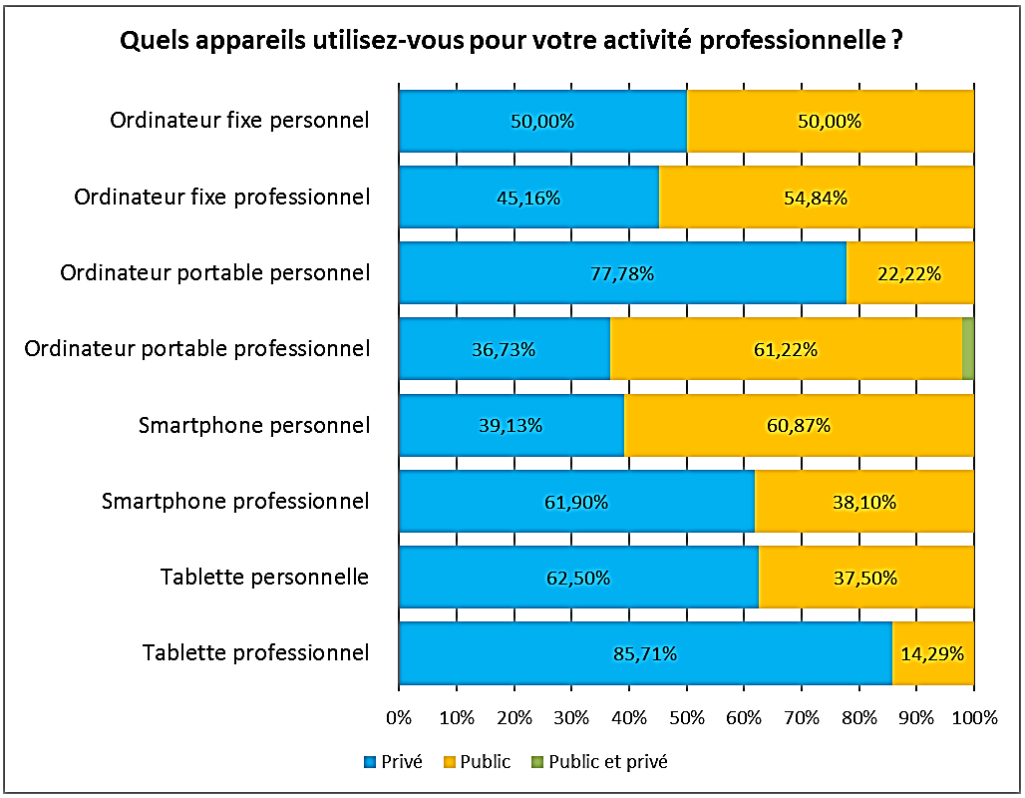
ID n° 119 Avez-vous un ordinateur à votre domicile équipé d'un antivirus ?



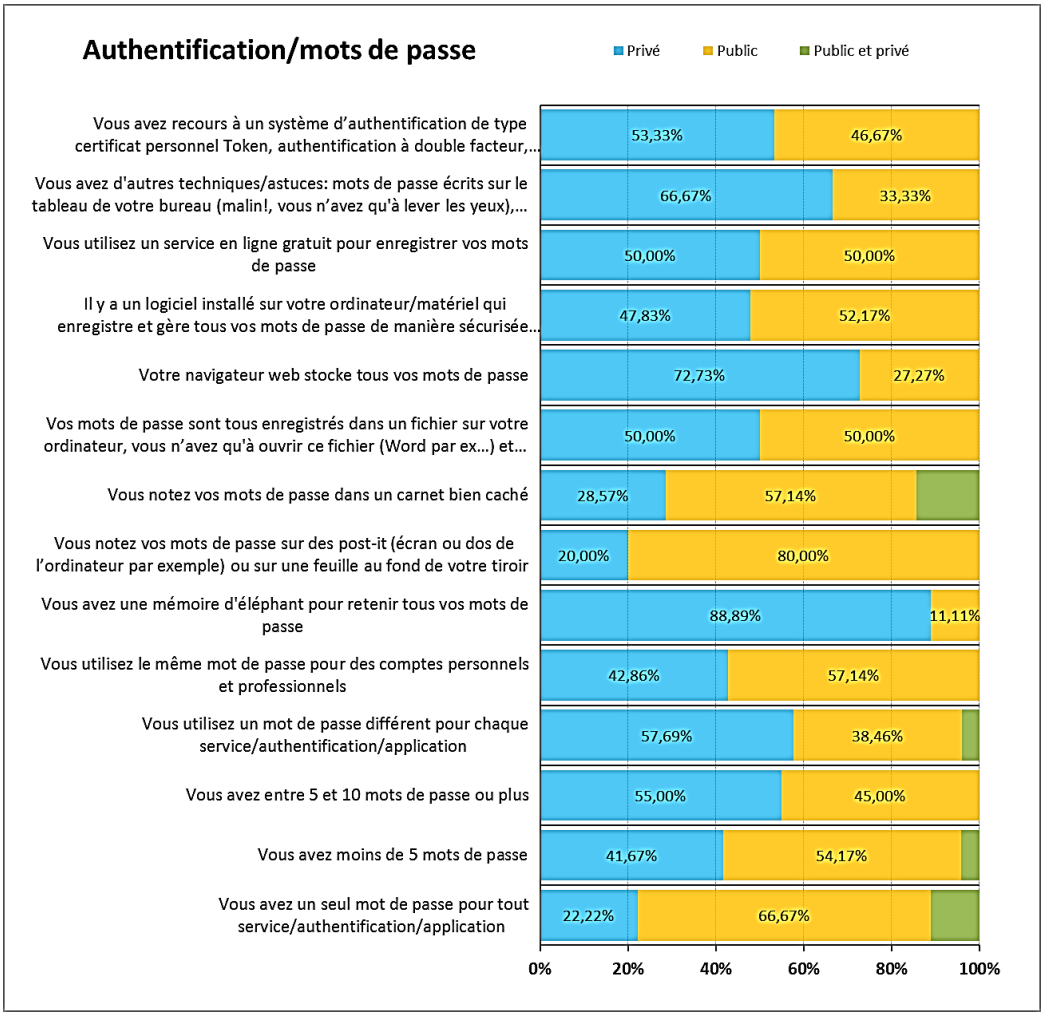
ID n° 120 Partage de mot de passe



ID n° 121 Que faites-vous en déplacement ?



ID n° 122 Quels appareils (professionnels ou personnels)



ID n° 123Autorisation et mot de passe

Annexe n°20 Suivi en temps réel des attaques

ÉDITEUR	LIEN
Cisco Security Web site	https://www.talosintelligence.com/
Digital Attack Map Top daily DDoS attacks worldwide	http://www.digitalattackmap.com Digital Attack Map est une visualisation de données en direct des attaques DDoS à travers le monde, construite grâce à une collaboration entre Google Ideas et Arbor Networks.
Norse surveillance	http://map.norsecorp.com/#/ Le spécialiste de la cyber sécurité Norse a créé une carte du monde où l'on peut voir en temps réel les attaques lancées contre l'un de ses honeypots319. Un spectacle presque hypnotisant, mais dont la violence incessante fait également froid dans le dos.
World Cyber Threat Map	https://threatmap.checkpoint.com/ThreatPortal/livemap.html
HTTPCS	https://map.httpcs.com/ HTTPCS (Hypertext Transfer Protocol Certified Secure) est un scanner automatisé de détection de vulnérabilités et de failles de sécurité dans les applications web, les sites web et les SaaS.

319 Le terme de **honeypot** ou, en français, de système " pot de miel " est un principe consistant à utiliser des systèmes pour attirer et piéger les pirates informatiques par la ruse, afin notamment de collecter des informations sur leurs méthodes.

ÉDITEUR	LIEN
Le décodeur	https://www.ledecodeur.ch/2014/05/25/carte-suivre-en-direct-les-cyber-attaques/
Kaspersky	https://cybermap.kaspersky.com/fr/
Fire Eyes	https://dothazard.com/carte-mondiale-des-cyberattaques-en-temps-reel-fire-eye/
Deutsche Telekom	http://www.sicherheitstacho.eu/?lang=en Site sicherheitstacho.eu affiche une mappemonde avec des pays de couleurs différentes, selon la fréquence des cyberattaques. Il affiche ainsi les événements quand ils se produisent, avec le moment précis de l'attaque, le pays d'origine et la cible visée.

ID n° 124 attaques en temps réel

Annexe n°21 les cert (computer emergency response team)

CERT/ CSIRT		URL
Cert Carnegie Mellon university		http://www.kb.cert.org/vuls/
Cert-fr	CSIRT dédié au secteur de l'administration française	http://www.cert.ssi.gouv.fr/
Cert-Devoteam	CSIRT commercial français	http://www.cert-devoteam.com/
Cert-ist	CSIRT dédié au secteur de l'Industrie, des Services et du Tertiaire (IST). Il a été créé à la fin de l'année 1998 par quatre partenaires : Alcatel, le CNES, ELF (Total) et France Télécom (Orange) ;	http://www.cert-ist.com/
Cert la poste	CSIRT du groupe La Poste, pour ses services internes et ses clients	http://www.trusted-introducer.org/directory/teams/cert-la-poste.html
Cert-lexsi (laboratoire d'expertise en sécurité informatique)	CSIRT commercial français	http://www.lexsi.fr/
Cert renater	CERT dédié à la communauté des membres du GIP RENATER (Réseau National de télécommunications pour la Technologie, l'Enseignement et la Recherche).	https://services.renater.fr/ssi/cert/avis
Cert-société général	CSIRT dédié au groupe Société Générale	http://cert.societegenerale.com/
Csirt-BNP Paribas	CSIRT dédié au groupe BNP Paribas	http://www.trusted-introducer.org/directory/teams/csirt-bnp-paribas.html
Orange-Cert-cc	CERT interne de l'opérateur de télécommunication Orange,	http://www.first.org/members/teams/orange-cert-cc
Cert-Wavestone	CSIRT commercial français	https://www.wavestone.com/fr/offre/cybersecurite-confiance-numerique/cert-w/
Cert crédit agricole	CSIRT dédié au groupe Crédit Agricole	http://www.trusted-introducer.org/directory/teams/cert-credit-agricole.html
Airbus cybersecurity and computer emergency response team	CSIRT commercial européen	http://www.cybersecurity-airbusds.com/
Cert banque de France	CSIRT interne de la Banque de France	https://cert.banque-france.fr/static/index.html
Csirt ATOS	CSIRT commercial français	http://www.trusted-introducer.org/directory/teams/csirt-atos.html

CERT/ CSIRT		URL
Airbus group Cert (ou aig Cert)	CSIRT du groupe Airbus	http://www.trusted-introducer.org/directory/teams/aig-cert.html
Cert capgemini-sogeti	CSIRT commercial français	http://www.sogeti.com/solutions/cybersecurity/cert
Cert sekoia	CSIRT commercial français	https://www.trusted-introducer.org/directory/teams/cert-sekoia.html
Cert ubik	CSIRT commercial français	http://www.digitalsecurity.fr/service/cert-ubik/index.html
Cert caisse des dépôts	CSIRT du Groupe Caisse des Dépôts	https://cert.caissedesdepots.fr/CERT
Cert Osiris	CSIRT de l'Université de Strasbourg	https://services-numeriques.unistra.fr/les-services-aux-usagers/services-osiris/cert-osiris.html
Cert Xerox	CSIRT commercial français	https://security.business.xerox.com/en-us

ID n° 125 les cert (computer emergency response team)

Annexe n°22 Le prix des données personnelles sur le darkweb

Les cybercriminels s'engouffrent dans cette voie pour piller les données, les contacts et surveiller l'activité des utilisateurs afin de revendre ces informations[320] sur le darknet[321].

Selon le pays et la qualité des données, les coordonnées de cartes bancaires se négocient entre 4 et 40 euros. Les cybercriminels peuvent aussi acheter des identifiants de comptes bancaires et de services de paiement en ligne. Le tarif est déterminé en fonction du solde du compte piraté. Cela va d'une vingtaine d'euros, pour acheter un compte crédité de quelques centaines d'euros, jusqu'à 260 euros pour un compte possédant 7 000 euros.[322]

Le pirate d'Instagram a créé une boutique dans le darknet pour écouler sa marchandise. Baptisée « *Doxagram* », elle est uniquement accessible par le navigateur Tor et propose les données pour 10 dollars par compte piraté. Il propose également, une vente par lot à prix négocié. Ce site référence les données personnelles par exemple de Justin Bieber et Kirsten Dunst.[323]

320 Instagram : des cybercriminels vendent le numéro de Taylor Swift pour 10 dollars http://www.zdnet.fr/actualites/instagram-des-cybercriminels-vendent-le-numero-de-taylor-swift-pour-10-dollars-maj-39856778.htm et

321 Un darknet est un réseau privé virtuel dont les utilisateurs sont considérés comme des personnes de confiance http://www.cil.cnrs.fr/CIL/spip.php?article2027

322 http://www.lefigaro.fr/secteur/high-tech/2014/12/08/32001-20141208ARTFIG00080-comment-s-enrichissent-les-pirates-du-web.php?redirect_premium

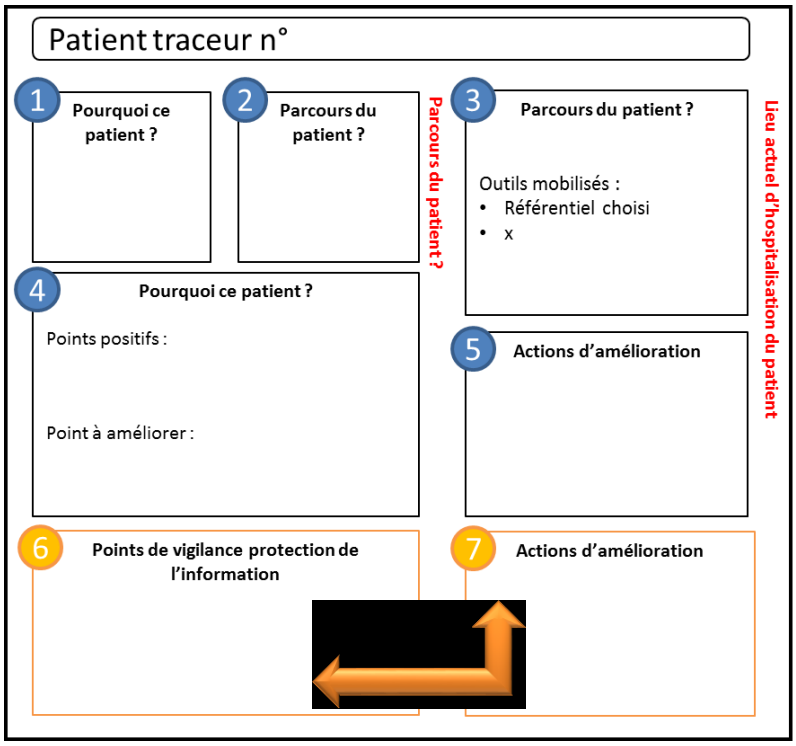
323 http://www.01net.com/actualites/les-donnees-de-6-millions-de-comptes-instagram-en-vente-sur-le-darknet-1247768.html

Annexe n°23 Les quatorze impacts d'une cyberattaque

Figure 4 Les quatorze impacts d'une cyberattaque Source deloitte.com

Annexe n°24 Trame d'une fiche pour la restitution des patients traceurs

Une zone (en orange point 6 et 7) a été ajoutée à la fiche « patient traceur », habituelle, relevant les points de vigilance sur la protection de l'information et les points d'amélioration à mettre en œuvre :



ID n° 126 : Trame d'une fiche pour la restitution des patients traceurs

Annexe n°25 Budget prévisionnel de la campagne de sensibilisation du GHT

	CHARGES ANNEE 1	CHARGES ANNEES SUIVANTES
Tous les collaborateurs (~ 5 300 personnes)	31 J.H. + 10 000 € 20 minutes par participant, soit 100 heures au total	18 J.H. + 10 000 € 20 minutes par participant, soit 100 heures au total
Directeurs & Secrétariat général (~ 20 personnes)	5 J.H. 40 minutes par participant, soit 13 heures au total	2,5 J.H. 20 minutes par participant, soit 7 heures au total
Métiers sensibles (Achats, RH, Soins, Finances, Techniques, SI, Biomédicale) (~ 100 personnes)	7 J.H.	1 J.H.
Finance (~ 10 personnes)	3 J.H. Une heure par participant, soit 10 heures au total	3 J.H. Une heure par participant, soit 10 heures au total
DSI Sécurité (~ 5 personnes)	2 J.H. Une heure par participant, soit 5 heures au total	2 J.H. Une heure par participant, soit 5 heures au total
Acteurs du PCA (~ 50 personnes)	24 J.H. 4 heures par participant, soit 200 heures au total	22 J.H. 4 heures par participant, soit 200 heures au total
DSI/Biomédical (30 personnes)	5 J.H. Une heure par participant, soit 30 heures au total	0,5 J.H. Une heure par participant, soit 30 heures au total
TOTAL	**77 J.H. + 10 000 €** **350 heures pour les participants, soit un peu plus d'une heure en moyenne par participant**	**93,4 J.H. + 10 000 €** **350 heures pour les participants, soit un peu plus d'une heure en moyenne par participant**

Annexe n°26 Évaluation budgétaire de la campagne du cabinet Carmignac

CIBLES	CHARGES ANNEE 1	CHARGES ANNEES SUIVANTES
Tous les collaborateurs (~ 300 personnes)	31 J.H. + 10 000 € 20 minutes par participant, soit 100 heures au total	18 J.H. + 10 000 € 20 minutes par participant, soit 100 heures au total
Top Management & Secrétariat général (~ 20 personnes)	5 J.H. 40 minutes par participant, soit 13 heures au total	2,5 J.H. 20 minutes par participant, soit 7 heures au total
Métiers sensibles (~ 100 personnes)	9 J.H.	3 J.H.
Comptabilité & commerciaux clientèle privée (~ 20 personnes)	3 J.H. Une heure par participant, soit 20 heures au total	3 J.H. Une heure par participant, soit 20 heures au total
Office Management (~ 10 personnes)	8 J.H. Une heure par participant, soit 10 heures au total	8 J.H. Une heure par participant, soit 10 heures au total
Commerciaux (~ 80 personnes)	Déjà comptabilisé dans « tous les collaborateurs E-Learning »	
Acteurs du PCA (~ 50 personnes)	24 J.H. 4 heures par participant, soit 200 heures au total	22 J.H. 4 heures par participant, soit 200 heures au total
Core Technologies (30 personnes)	5 J.H. Une heure par participant, soit 30 heures au total	0,5 J.H. Une heure par participant, soit 30 heures au total
TOTAL	85 J.H. + 10 000 € 350 heures pour les participants, soit un peu plus d'une heure en moyenne par participant	57 J.H. + 10 000 € 350 heures pour les participants, soit un peu plus d'une heure en moyenne par participant

ID n° 127 évaluation budgétaire

Annexe n°27 Communication ponctuelle dans le cadre de la sensibilisation

TYPE	SOCIETE	OUTILS	COUT	EFFICACITE	PERSONNALISATION
Serious game	MAVI INTERACTIVE http://www.maviinteractive.com/ Démonstration sur https://vimeo.com/46310970	Modules SSI réutilisables	Moyen (~10K€ + coût de personnalisation si nécessaire)	Forte	Faible
	ŒIL POUR ŒIL GAMIFICATION https://www.oeilpouroeil.fr/	Jeux adaptés au contexte, à créer de bout en bout	Elevé (30k € à 50K€ pour 30 minutes de modules)	Forte	Forte
Saynètes avec questionnaire	CONSCIO TECHNOLOGIE https://www.conscio-technologies.com/ Démonstrations sur https://youtu.be/xWpv_yAtAYU	Modules « protection des données » et « Sécurité SI » réutilisables	Moyen (~10k € pour 2 modules)	Forte	Faible
Diapositives avec questionnaire	ELUCIDAT https://www.elucidat.com/	Diapositives suivies de questionnaires, sur web ou ordiphone	Moyen	Moyenne	Forte
	BEEDEEZ https://www.beedeez.com/				
Formation en ligne spécial santé	Pour les adhérents à la centrale d'achat CAIH, réservée aux établissements de santé, un module de formation en ligne sur la sécurité du système d'information hospitalier http://www.caih-sante.org/ est proposé. La société https://www.ktm-advance.com/ est détentrice de la marche.	Module adapté à la santé	Pour un seul marché de 0,40 € HT par lit de l'établissement, avec un plafond annuel de 1 000,00 € HT.		

Annexe n°28 Message accompagnant le premier document de la campagne du cabinet Carmignac

ID n° 128 support de campagne de sensibilisation en français

Annexe n°29 Les types d'Attaques et menaces

On distingue plusieurs types d'attaques :

VER

Les tout premiers vers sont apparus en 1982. Un des plus connus est « I love you » en mai 2000.
« Slammer » fait son apparition en 2002-2003, qui a provoqué un ralentissement mondial d'internet. Certains aéroports américains ont dû reporter ou annuler des vols. Des dégâts économiques ont été évalués à 1 milliard de dollars.

VIRUS

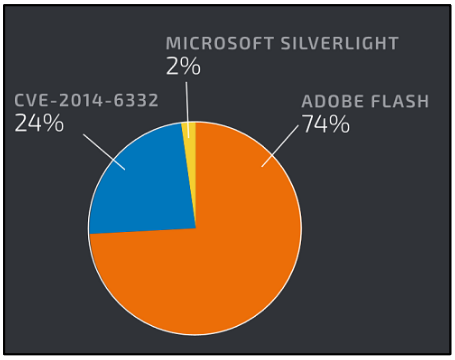
10000 nouveaux virus ont été identifiés en 2004 comme MyDoom[324], le système d'exploitation Windows était visé afin de lancer des attaques de dénis de service.
Rançongiciel ou ransomware
Certaines demandes de rançon peuvent s'élever jusqu'à 1 000 dollars selon le directeur de l'ANSSI.
Les pirates ne manquent pas d'imagination, sont machiavéliques et s'adaptent au nouveau mode économique comme le SAAS (Software As A Service). Ils incitent les victimes à infecter d'autres utilisateurs pour échapper au paiement de leur rançon (ransomware PopCorn Time) ou proposent des ransomware « clefs en main » comme le ransomware Satan en mode SAAS.
Un vrai défi pour les responsables de la sécurité : se mettre dans la peau de l'ennemi pour inventer, en même temps que lui de nouvelles protections ! Pour ça il faut connaître son ennemi.
Cisco a évalué le « chiffre d'affaires » à 34 millions de dollars bruts annuels d'un réseau de cyber criminels en 2016.
Angler Kit : Cisco débusque un groupe de cybercriminels d'envergure[325]

---

[324] MyDoom.A ou Novarg.A est un virus informatique qui se propage par les courriels ou le service P2P de Kazaa. Les premières infections ont eu lieu le 26 janvier 2004. Le virus est aussi appelé : Mimail.R ou Shimgapi. Il affecte le système d'exploitation Microsoft Windows. Source https://fr.wikipedia.org/wiki/MyDoom.A

[325] http://www.zdnet.fr/actualites/angler-kit-cisco-debusque-un-groupe-de-cybercriminels-d-envergure-39826128.htm

Cisco publie une étude portant sur un groupe de cybercriminels ayant intensivement eu recours à l'Angler Exploit Kit, une suite logicielle servant à infecter les machines via de multiples failles de sécurité. Sans surprise, les données récoltées par Cisco et Talos révèlent que le cyber crime paie plutôt bien.
Cisco explique ainsi que 75 % des vulnérabilités exploitées par l'Angler exploit kit sont des vulnérabilités affectant Flash, suivi par 24 % exploitant une autre faille connue au sein d'Internet Explorer.
En s'appuyant sur ces chiffres, les chercheurs de Cisco, au sein de Talos[326], ont tenté d'évaluer le retour sur investissement d'un seul serveur exploitant ce type de schéma. Ils expliquent avoir observé qu'un seul serveur faisant fonctionner Angler Exploit kit visait 9 000 victimes par jour et parvenait à en infecter environ 40 %. La demande de rançon moyenne étant évaluée à 300 dollars, les chercheurs de Cisco estiment que les membres de ce groupe particulier de cybercriminels parvenaient à amasser au total 30 millions de dollars par an, au vu de la taille de leurs activités et du nombre de machines déployées. On prendra le chiffre avec des gants : de l'aveu même de Cisco, nombre de variables restent inconnues dans l'équation : le nombre de rançons effectivement payées et les sommes exactes restent encore flous, ainsi que la taille totale de l'infrastructure utilisée par ce groupe d'attaquants.



ID n° 129 La répartition des failles de sécurité exploitées par l'Angler Exploit Kit parmi les données récoltées par Cisco

Annexe n°30 Attaques et vulnérabilités humaines

Dans la typologie des menaces, le facteur humain est essentiel et se matérialise sous plusieurs formes :

TYPE D'ATTAQUE	EXPLICATION
L'ingénierie sociale **Compromission de la messagerie en entreprise (BEC, Business Courriel Compromise)** **L'arnaque au président ou escroquerie aux faux ordres de virement (FOVI)**	Afin de contourner des systèmes de protection, ou d'obtenir des informations normalement confidentielles, un attaquant peut tenter d'abuser de la naïveté d'un utilisateur peu sensibilisé ; Un courriel frauduleux va inciter un employé de faire des virements bancaires ou à transmettre des informations confidentielles sur l'entreprise. Ces messages semblent provenir du Directeur/PDG ou d'un cadre supérieur. Le pirate exhorte la personne de ne pas parler de cette opération à personne dans son entourage. Les préjudices identités, entre 2010 et 2016, représentent 485 millions d'euros et 2 300 plaintes déposées[327]. Le volume des BEC est passé de 1 % en 2015 à 42 % fin 2016[328]
La manipulation d'individus	MICE (Money, Ideology, Compromise, Ego). Cet acronyme anglophone résume les différents moyens pouvant permettre de s'assurer le concours de quelqu'un. Qu'il soit attiré par l'argent, une idéologie commune (religieuse ou politique), sous l'emprise d'une compromission ou de son ego, un individu peut être manipulé.
Vol d'information **Phishing** **Vishing**	Les attaquants essaient de duper les employés à l'aide de courriers électroniques. Ils peuvent récupérer des organigrammes, des noms et des mots de passe pour accéder au système. Les pirates commencent par récupérer des adresses de messagerie à partir de publications accessibles du grand public, de réseaux sociaux et font des hypothèses de messageries à partir du nom de l'entreprise (exemple : nom.prénom@société.com). Après quoi des offres séduisantes arrivent dans ces boîtes aux lettres ou ces malfrats se font passer pour un fournisseur ou le service informatique, orientant les utilisateurs, avec un message convaincant, vers un lien à cliquer. Exemple : comme « notre boîte est arrivée à sa limite, cliquez ici ou répondez à ce message pour demander au département informatique d'augmenter la taille de notre boîte de réception » ou d'autre message. Ces personnes malveillantes sont parfois plus subtiles et adresse des messages du type : « En tant qu'administrateur du programme de primes de l'entreprise, je tiens

326 https://www.talosintelligence.com/angler-exposed/
327 Police nationale, https://www.police-nationale.interieur.gouv.fr/Actualites/Dossiers/Cybercrime/L-arnaque-au-president-ou-escroquerie-aux-faux-ordres-de-virement-FOVI, 21/01/2016
328 Proofpoint, édition 2017 du rapport « Le facteur humain »

TYPE D'ATTAQUE	EXPLICATION
	à attirer notre attention sur les modifications que nous allons bientôt apporter au programme. Cliquez ici pour consulter les détails avant que nous ne planifiions un bref entretien téléphonique. » Certains utilisateurs, peu méfiants répondent, et parfois entament une conversation avec l'auteur de l'attaque qui va abuser de sa crédulité pour lui extorquer encore plus d'informations. Il existe aussi le vishing (combinaison de voice et phishing) qui est le même procédé par téléphone. Les personnes visées sont soit contactées par un automate soit par une personne physique.329 Le but du phishing est de tromper les internautes afin qu'ils donnent des informations confidentielles comme un numéro de carte bancaire, un mot de passe… Ces informations sont utilisées pour extorquer de l'argent aux victimes. Les criminels utilisent, afin de masquer leur identité, des réseaux de robots ordinateurs (botnets) ou zombies. Des ordinateurs de particuliers peuvent être utilisés, comme relais, sans qu'ils le sachent à des fins criminelles. Un réseau peut être constitué de 3 000 à 10 000 ordinateurs zombies.
Longlining	Courriels frauduleux personnalisés inspirés par des campagnes marketing. Ces messages passent à travers les antispams (antipourriel) ou analyse de contenu et ne contiennent pas de pièce jointe.
Attaque « Watering Hole » (ou « point d'eau »)	Il s'agit de compromettre des sites web stratégiques et d'y attirer, par la ruse ou des courriels, certaines personnes qui seraient intéressées par les informations diffusées, comme une oasis, mais sans eau !
Money muling	Il s'agit de blanchiment d'argent. Un malfrat vole de l'argent ou des biens par l'intermédiaire de malware ou hameçonnage, de trafic de stupéfiant et recrute, habilement, des internautes pour transférer cet argent via leur compte bancaire et contre rétribution.330
Pourriel vocal ou Ping call	Notre téléphone sonne une seule fois et cela raccroche. L'escroc espère que vous rappeliez ce correspondant car il s'agit d'un numéro de téléphone surtaxé. Cela arrive sur les portables et les lignes fixent.
SMS frauduleux	Le but est le même que le Ping Call, allécher le propriétaire d'ordiphone à répondre au numéro indiqué, par un message alléchant (exemple : Nous avons gagné à la loterie). Certains escrocs rentabilisent leur investissement en revendant des numéros de téléphone de personnes qui ont répondu au message. Ceux-ci étant le plus à même à se faire abuser à nouveau.
Cyberattaque des ordiphones	Cela commence par un SMS commercial invitant la victime à procéder à une mise à jour payante d'une application. Les pirates informatiques utilisent les coordonnées bancaires immédiatement après que l'utilisateur a saisi l'information.

ID n° 130 attaques humaines

329 Police Nationale, https://www.police-nationale.interieur.gouv.fr/Actualites/Dossiers/Cybercrime/Le-vishing-hameconnage-vocal-gare-aux-appels-frauduleux, 20/01/2015

330 Police Nationale : https://www.police-nationale.interieur.gouv.fr/Actualites/Dossiers/Cybercrime/Money-muling-ne-vous-mettez-pas-dans-de-beaux-draps, 28 novembre 2017

BIBLIOGRAPHIE

LIVRES

1. Monique Dagnaud, « Génération Y : Les jeunes et les réseaux sociaux, de la dérision à la subversion », Nouveaux Débats, Presses de Sciences Po (P.F.N.S.P.), 2011
2. Noyé, Didier, Piveteau, Jacques Editeur, « Concevoir, animer, évaluer une formation », INSEP Consulting édition, 2005
   - Chapitre 6 Les aides pédagogiques leur rôle et comment les utiliser à quelles fins.
   - Chapitre 13 - Le développement de la formation en ligne p167
3. Philippe Bernier, « Toute la fonction Formation : Savoirs. Savoir-être. Savoir-faire », Dunod, 2015
   - Chapitre 2 L'ingénierie de la formation : L'ingénierie de la formation permet de déterminer les déférentes étapes concourant à la mise en œuvre de la formation au sein de l'organisation. Se savoir théorique constitue un fondement de l'approche de la politique formation.
4. Christophe Parmentier, « Tout pour réussir dans le métier de formateur. Les fondamentaux du métier, Les meilleures pratiques et les outils, Le quotidien du métier L'évaluation et le suivi d'activité » Eyrolles, 2014
   - Chapitre 2 Des adultes en formation : l'andragogie
   - Chapitre 3 Les concepts clés de la formation des adultes
   - Chapitre 4 La formation ouverte et l'e-learning
   - Chapitre 7 Après : l'évaluation des participants à la formation
5. Franck Jullien « Découvrir sa personnalité… et celles des autres », Eyrolles 2012 (2e édition)
6. Yves Chaumette, « La qualité au-delà des mots : perception par la couleur », Hermès science, 2006
7. Aumont B., Mesnier P.-M, « L'acte d'apprendre » L'Harmattan 3e édition, 2006
8. Mémento de l'évaluation : Analyser et améliorer sa pratique de l'évaluation (édition 2014) - Auteur : Galiana, Dominique Editeur : Educagri Editions Publication : 2014
9. Robert-Vincent Joule et Jean-Léon Beauvois, « Petit traité de manipulation à l'usage des honnêtes gens », mars 2014
10. Arnaud Tonnelé, « 65 outils pour accompagner le changement individuel et collectif », Eyrolls 2016
11. Laurent Bloch Christophe Wolf Hugel, « Sécurité informatique Principes et méthode », Eyrolles 2007. Pages 37 et 38,
12. Jean François Challande, Jean Louis Lequeux, « Le Grand Livre du DSI, Mettre en œuvre la direction du système d'information 2.0 », Eyrolles, 2009. Chapitre 9 implications des utilisateurs dans la sécurité,
13. CNIL/RGDP : Fabrice Mattatia, « Le droit des données personnelles N'attendez pas que la CNIL ou les pirates vous tombent dessus ! », Eyrolles, 2016
14. C. Morley, M. Bia-Figueiredo et Y. Gillette, Processus métier et S.I. Dunod 3e édition 2011
15. CDSE (Club des Directeurs de Sécurité des Entreprises). Protection de l'information : Pourquoi et comment sensibiliser (French Edition) Editions L'Harmattan. Édition du Kindle.

ARTICLES

16. Statistiques et infographie https://fr.statista.com/
17. WannaCry
    - https://fr.sputniknews.com/international/201705251031524729-cyberattaque-economie-mondiale/
    - http://www.liberation.fr/futurs/2017/05/13/au-royaume-uni-recuperation-apres-la-cyberattaque-contre-les-hopitaux_1569310
    - https://www.undernews.fr/reseau-securite/rapport-radware-ert-2017-les-attaques-contre-le-secteur-public-en-hausse-les-botnet-iot-a-craindre.html
18. Locky https://korben.info/locky-quil-y-a-a-savoir-malware-moment.html
19. NotPetya (autrement appelé NotPetya, Petna, ExPetr) http://www.silicon.fr/poupard-anssi-notpetya-medecine-guerre-179807.html?inf_by=59b2859a671db83a168b49d2
20. Article : recherche de l'Institute for Color Research (une division de Color Communications INC.) menée en collaboration avec l'Université de Winnipeg https://www.colorcom.com/
21. OSSIR (Observatoire de la Sécurité des Systèmes d'Information et des Réseaux) https://www.ossir.org/resist/supports/cr/2017/2017-06-20/Predation_informationnelle.pdf
22. Articles du webmagazine « Limait »
    - http://www.lemagit.fr/actualites/450426264/Faire-des-utilisateurs-les-yeux-et-les-oreilles-de-la-fonction-securite
    - http://www.lemagit.fr/actualites/2240189167/Les-programmes-de-sensibilisation-a-la-securite-informatique-ont-une-vraie-valeur
    - http://www.lemagit.fr/actualites/4500255630/Securite-des-systemes-dinformation-comment-sensibiliser-tous-les-acteurs-de-lorganisation
23. Article : étude KPMG, « Les établissements de santé : en l'espace d'un an, et malgré une actualité forte et anxiogène la cyber sécurité est passée de la première à la cinquième place des priorités des organisations » http://itsocial.fr/metiers/direction-generale/pdg-ont-chemin-a-faire-de-prendre-cybersecurite-serieux/
24. ITSOCIAL.FR Le coût moyen du ransomware est passé à 1 077 $. http://itsocial.fr/enjeux-it/securite-dsi/cybersecurite/cout-moyen-ransomware-passe-a-1-077/
25. D'où vient la cybercriminalité ? Les origines et l'évolution de la cybercriminalité https://www.le-vpn.com/fr/cybercriminalite-origines-evolution/
26. Qu'est-ce qu'un ransomware ? Les 5 meilleurs articles sur les ransomwares : http://itsocial.fr/enjeux-it/securite-dsi/cybersecurite/quest-cybersecurite-5-meilleurs-articles-cybersecurite/
27. Gérard Peliks, « La certification critères communs expliquée à ceux qui croient encore à la sécurité subjective », Security Center of Competence EADS Defence and Security, Août 2007 https://www.forumatena.org/files/livresblancs/Whitepaper-Criteres-Communs.pdf
28. La rédaction de www.techniques-ingenieur.fr « Comment évaluer l'efficacité des mesures de sécurité d'un SMSI ? », http://www.techniques-ingenieur.fr/actualite/informatique-electronique-telecoms-thematique_193/comment-evaluer-l-efficacite-des-mesures-de-securite-d-un-smsi-article_4662/, 25 mars 2009,
29. La société TrapX Security a réalisé une étude sur les cyber-attaques dirigées et détectées par les établissements de santé entre fin 2015 et début 2016. TrapX Labs - A Division of TrapX Security, INC. Date : May 7, 2015
    - https://www.objetconnecte.com/dispositifs-medicaux-attaques-2806/
    - http://trapx.com/wp-content/uploads/2017/08/AOA_Report_TrapX_MEDJACK.2.pdf
    - http://trapx.com/wp-content/uploads/2017/08/AOA_Report_TrapX_AnatomyOfAttack-InternetOfThings.pdf

- https://vimeo.com/212149970

30. Une pédiatre de L'AP-HM condamnée pour traitement illicite de données de santé : https://secureidees.com/2017/09/18/une-pediatre-de-lap-hm-condamnee-pour-traitement-illicite-de-donnees-de-sante/
31. Traitement et hébergement illicite de données de santé https://secureidees.com/2017/09/15/traitement-et-hebergement-illicite-de-donnees-de-sante/
32. Source les Echos : Données personnelles : Facebook condamné https://www.lesechos.fr/tech-medias/hightech/021209472391 2-donnees-personnelles-facebook-condamne-2087308.php
33. Cybercriminalité : l'insuffisante prise de conscience des pouvoirs publics http://www.lefigaro.fr/vox/societe/2017/05/19/31003-20170519ARTFIG00272-cybercriminalite-l-insuffisante-prise-de-conscience-des-pouvoirs-publics.php
34. La politique cible des pirates informatiques
    - http://www.securityweek.com/hackers-target-ukraines-election-website
    - http://edition.cnn.com/2016/06/21/politics/dnc-hack-russians-guccifer-claims/
    - http://www.lemonde.fr/pixels/article/2016/12/21/des-attaques-informatiques-a-visee-politique-envisageables-en-france_5052650_4408996.html
    - http://www.lepoint.fr/presidentielle/presidentielle-2017-l-election-menacee-par-une-cyberattaque-russe-08-02-2017-2103415_3121.php
    - http://www.europe1.fr/politique/une-cyber-attaque-russe-sur-le-second-tour-de-la-presidentielle-tout-est-plausible-mais-3311300
35. Article : « L'ordinateur est complètement con » « Fondamentalement, l'ordinateur et l'homme sont les deux opposés les plus intégraux qui existent. ».
    - Entretien avec Gérard Berry, informaticien et professeur au Collège de France, médaille d'or 2014 du CNRS. Par Xavier de La Porte. L'observateur le 10 juin 2017. http://tempsreel.nouvelobs.com/rue89/rue89-le-grand-entretien/20160826.RUE7684/gerard-berry-l-ordinateur-est-completement-con.html

MEMOIRES/THESES

36. L'usage des technologies de l'information et de communication dans la pratique de l'infirmière, mémoire de fin d'étude de Michel Alice 2014.
37. Informations sur les procédures de contrôle interne, les facteurs de risques et les conflits d'intérêts du Crédit Agricole des Savoie Exercice 2013 AFCDP (http://www.afcdp.net/Theses-et-Memoires-Informatique)
38. Sécurité du système d'information : un enjeu majeur pour la France, LASBORDES Pierre, La Documentation française Collection des rapports officiels janvier 2006
39. Gestion des identités et des accès pour le système d'information du CNRS Cryptographie et sécurité [cs. CR], Guillaume Harry. 2013. (dumas-01142992) https://dumas.ccsd.cnrs.fr/dumas-01142992
40. L'e-santé, un domaine émergent nécessitant un accompagnement spécifique, Yohan Dubedout, IEP de Toulouse 2015 https://memoires.sciencespo-toulouse.fr/uploads/memoires/2015/5A/memoire_DUBEDOUT-YOHAN-MzYyNjYyNjI=.pdf
41. Gestion des identités et des accès pour le système d'information du CNRS Cryptographie et sécurité [cs. CR], Guillaume Harry. 2013. < dumas-01142992 > https://dumas.ccsd.cnrs.fr/dumas-01142992/document

GUIDES / ETUDES / RAPPORTS PROFESSIONNELS

42. Upbraining, comment leur apprendre à apprendre. Cette méthode a été développée par le professeur Feuerstein et son équipe à l'institut Feuerstein pour le développement du potentiel d'apprentissage (http ://www.icelp.info) à Jérusalem et proposée par Christine Mayer et l'association J'AVANCE et de l'institut Upbraining.
43. Etude sur l'usage des téléphones mobiles dans le monde et les perspectives Ericsson Mobility Report Juin 2017 EAB-17 : 005964 Uen, Revision B Ericsson AB 2017 https://www.ericsson.com/assets/local/mobility-report/documents/2017/ericsson-mobility-report-june-2017.pdf
44. Etude : Deloitte, « Cyberattaques : comment chiffrer les impacts ? Le visible et l'invisible » https://www2.deloitte.com/fr/fr/pages/risque-compliance-et-controle-interne/articles/cyberattaques-chiffrer-les-impacts.html
45. Rapport : Accenture, « Cost of cyber crime study 2017 insights on the security investments that make a difference », Ponemon institute, 2017 https://www.accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf
46. L'édition 2016 du rapport Data Breach Investigations Report de Verizon
47. Enquête effectuée en 2017 par la HIMSS (Healthcare Information and Management Systems Society) sur la cybersécurité,
48. Etude : « *Crossing the Line* » réalisée par KPMG mai 2017
49. Sandrino de 1blink.fr, « Pourquoi et comment sensibiliser ses utilisateurs à la sécurité » (1blink est une société de conseil en Sécurité des Systèmes d'Information), 31 décembre 2015
50. Bilan Cert-IST (Industrie service tertiaires) 2016 des failles et attaques
51. Délégation ministérielle aux industries de sécurité et à la lutte contre les cybers menaces, « état de la menace liée au numérique en 2017, Rapport n° 1 », janvier 2017
52. « Baromètre de la cybersécurité des organisations Vague 2 Club des Experts de la Sécurité de l'Information et du Numérique », Alain Bouillé, Emmanuel Kahn, Agathe Martini, OpinionWayjanvier 2017
53. BNP Paribas et The Boson Project publient l'étude « La Grande InvaZion », une enquête réalisée auprès de 3 200 jeunes français de 15 à 20 ans. 21 mai 2015
54. Les sciences économiques et sociales Enseignement et apprentissages Auteur (s) : Beitone, Alain, Dollo, Christine, Hemdane, Estelle. Editeur : De Boeck Supérieur Publication : 2017
55. Florent Côte, formation à la certification – le patient traceur, HAS V2014
56. « Référentiel de bonnes pratiques sur les applications et les objets connectés en santé (Mobile Health ou mHealth) », évaluation et amélioration des pratiques, HAS (Haute Autorité en Santé), octobre 2016,
57. AZIP SANTE : « Guide pratique Gestion des habilitations d'accès au système d'information Politique générale de sécurité des systèmes d'information de santé (PGSSI-S) V0.2 », mai 2016
58. Etat de la menace liée au numérique en 2017 - Rapport n° 1 – janvier 2017, partie 1 - Enjeux stratégiques : Coût de la cybercriminalité, 2017,
59. « Gouverner à l'ère du numérique : Le guide de la cyber sécurité pour les dirigeants d'organisation », Palo Alto et la Tribune et CESIN et Solutions numériques, Palo Alto Networks, 2016 Septembre
60. « La sécurité économique au quotidien en 22 fiches thématiques », Premier ministre délégation

interministérielle à l'intelligence économique, avril 2014,

61. « Le guide essentiel de la surveillance des activités et comptes à privilèges Introduction aux challenges des accès et comptes à privilèges et à leur surveillance », Balabit » juin 2017.
62. « Guide du RSSI de demain L'humain au cœur de la cyber sécurité : quand le RSSI se transforme » ALLIANCY LE MAG
63. « Guide de cyber sécurité édition 2016 », https://www.alliancy.fr/guide-cybersecurite-2016
64. Article : L'hôpital de Mâcon, vacciné contre les « virus » https://www.alliancy.fr/lnep/lhopital-de-macon-vaccine-contre-les-virus
65. « Le cyber risque dans la gouvernance de l'organisation, pourquoi et comment en parler en Comex ? » CIGREF, octobre 2016.
66. « Eduquer les acteurs de l'organisation aux risques numériques », 2011-2012
67. CLUSIF (club de la sécurité de l'information français), https://clusif.fr
68. « Rapport : Menaces Informatiques et Pratiques de Sécurité en France » - France édition Clusif
69. « Cellule de crises et système d'information », Clusif janvier 2017
70. L'AFAI (Association française de l'audit et du conseil informatiques), « Contrôle interne et système d'information 2e édition », 6 juillet V 2.2, 2008.
71. Légifrance https://www.legifrance.gouv.fr
72. ANAP (Agence Nationale d'Aide à la Performance) http://www.anap.fr
73. ATIH : Agence technique de l'information sur l'hospitalisation https://www.atih.sante.fr/
74. CNIL Commission nationale de l'informatique et des libertés https://www.cnil.fr/
75. Article juridique : Frédéric Forster Bensoussan Avocats Lexing, « Quel statut attribuer aux données ? » E.D.I N° 68 1er mai 2017 https://www.alain-bensoussan.com/wp-content/uploads/2017/05/34292572.pdf
76. Global security mag, Logical and physical security magazine https://www.globalsecuritymag.fr/
77. Institut national des hautes études de la sécurité et de la justice « Défis La revue du département Intelligence et sécurité économiques n° 7 »,
78. Hervé Schauer, « Gestion des incidents liés à la sécurité de l'information » Conférence Internationale Management de la Sécurité de l'Information selon la norme ISO/IEC 27001 Paris, 25 avril 2012 diapositive n° 9-12-13-15-16, 2012 ».
79. Protection des données, Jean-François Parguet, Les cahiers de L'iNria, la recherche – Normes
80. Bilan Cert-IST (Industrie service tertiaires) 2016 des failles et attaques
81. Mario Roy, Madeleine Audet, Johanne Archambault, Danielle St-Louis, « Créer une communauté stratégique pour favoriser le changement : une de cas portant sur l'organisation du travail dans le secteur de la santé », Gestion 2009/4 (Vol.34), HEC Montréal, pages 48 à 54
82. QERCI (questionnaire d'évaluation des risques pour le système d'information de sante système d'information, SSI et CNIL) https://www.apssis.com/upld/fichiers/Questionnaire-QERSI-S-v2.pdf
83. Lionel Bellenger, « La force de de persuasion. Du bon usage des moyens d'influencer et de convaincre », Collection formation permanente, Séminaires Muchielli ESF éditeur de. Exposé N° 3 les ressorts de l'influence
84. ANDRAGOGIE Support de cours de Sami HACHICHA institut supérieur de l'éducation et de la formation continue.
85. Karine Robinault, « Introduction à la didactique – Master Didactiques et Interactions » octobre 2006
86. Bourgeois E., Nizet J., « Apprentissage et formation des adultes » Presses Universitaires de France – PUF, 2005

SITE WEB

87. Site web : Le panorama des menaces informatiques en 2017 http://www.silicon.fr/hub/malwarebytes-hub/le-panorama-des-menaces-informatiques-en-2017?inf_by=59b24379671db8da448b480a
88. Site web : Evolution graphique http://evolutiongraphique.com/la-signification-cachee-des-couleurs-en-communication-visuelle/
89. Site web : Céline Design
    - https://www.celinedesign.com/blog/mettez-de-la-couleur-dans-vos-creations.php
    - Lorsque la couleur est bien utilisée, elle constitue un formidable outil de communication pour véhiculer des messages et susciter des émotions.
90. Site web : Toutes-les-couleurs Codes et nuanciers couleurs http://www.toutes-les-couleurs.com/
    - La couleur peut influencer nos émotions, nos actions ainsi que notre conception des choses des idées et des personnes. Une fois que l'on comprend certaines choses comme la signification et l'impression que donne une couleur, le rôle des couleurs complémentaires, l'association des couleurs et biens d'autres, on peut alors prévoir les résultats et comprendre l'effet que ces dernières produisent sur la cible.
91. D'où vient la cybercriminalité ? Les origines et l'évolution de la cybercriminalité https://www.le-vpn.com/fr/cybercriminalite-origines-evolution/

NORMES ET METHODES

92. Normes de sécurité : les méthodes d'analyse des risques : http://cyberzoide.developpez.com/securite/methodes-analyse-risques/
93. Capability Maturity Model Integration Source :
    - http://cmmiinstitute.com,
    - https://fr.wikipedia.org/wiki/Capability_Maturity_Model_Integration
94. Normes de sécurité : les méthodes d'analyse des risques : http://cyberzoide.developpez.com/securite/methodes-analyse-risques/
95. ADKAR Wikilean http://www.wikilean.com/Articles/Lean-6-Sigma-Management/3-Conduire-le-changement-14-articles/La-methode-ADKAR
96. Design Thinking
    - 3M Corporation : http://www.billiondollargraphics.com/infographics.html).
    - http://trendemic.net/etapesdesign-thinking.html
    - https://medium.com/a-road-to-design/les-fondamentaux-de-la-culture-design-thinking-a2a0ff370f20
    - https://www.lescahiersdelinnovation.com/2015/04/vers-la-mort-du-design-thinking/
    - http://www.lescahiersdelinnovation.com/2015/10/le-design-thinking-se-rapproche-t-il-du-coeur-des-organisations/.
97. Genba Walk (Comparaison ou approche similaire que le patient traceur)
    - https://leansixsigmafrance.com/blog/soyez-proche-du-terrain-avec-le-gemba-walk/
    - https://jpdconseil.com/excellence-organisationnelle-operationnelle-organisation/questions-gemba-walk/
98. EBIOS : La méthode EBIOS est une méthode d'évaluation des risques en informatique, développée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Elle est compatible avec les normes ISO 15408 (critères communs) et ISO 27002. EBIOS est utilisée dans le secteur public (l'ensemble des ministères et des organismes sous tutelle), dans le secteur privé (cabinets de conseil, petites et grandes organisations), en France et à l'étranger (Union européenne, Québec, Belgique, Tunisie, Luxembourg…).
99. Mehari (Méthode Harmonisée d'Analyse de Risques) est développée par le CLUSIF depuis 1995, elle est dérivée des méthodes Melissa et Marion. Existant en langue française et en anglais, elle est utilisée par de nombreuses organisations publiques ainsi que par le secteur privé. MEHARI respecte

les lignes directrices tracées par la norme ISO/IEC 27005 et permet une intégration dans une démarche complète qui permet d'être utilisée aussi dans le cadre d'un Système de Management de la Sécurité de l'Information (ISO/IEC 27001 : 2013) grâce à sa capacité à impliquer et sensibiliser la Direction de l'entité comme les responsables opérationnels.

TABLE DES FIGURES ET TABLEAUX