CYBERSÉCURITÉ

FAITES VRAIMENT

DE VOS UTILISATEURS

LE MAILLON FORT

DE VOTRE SI

conscio technologies

SOMMAIRE

CYBERSÉCURITÉ

FAITES VRAIMENT DE VOS UTILISATEURS
LE MAILLON FORT DE VOTRE SI

CONSCIO TECHNOLOGIES
12 rue Vivienne
75002 Paris - France

https://www.conscio-technologies.com
contact@conscio-technologies.com
+33 (0) 184 80 82 00

1. LES ENJEUX

Pratiquement pas une semaine ne passe sans que l'actualité ne se fasse l'écho d'un incident de sécurité majeur. L'étude « McAfee Labs Threats Report : août 2019 », qui présente l'activité cybercriminelle et l'évolution des cybermenaces au premier trimestre 2019, annonce 504 nouvelles menaces par minute lors de premier trimestre, avec une augmentation de 118 % des ransomwares. Fuite de données, systèmes bloqués par un ransomware, détournement de fonds, usurpation d'identité, sont autant de types d'attaques fréquemment rencontrés. Dans la grande majorité des cas, un défaut de comportement d'un ou plusieurs utilisateurs est en cause. Cela peut s'agir de celui qui clique sur e-mail de phishing permettant l'introduction d'un code malveillant. Cela peut s'agir aussi de celui qui utilise son mot de passe et son e-mail professionnels sur un site qui se fait pirater, offrant ainsi à des pirates les informations nécessaires pour se connecter au système d'information. Cela peut aussi être le cas de celui qui, trop naïf, se fait duper sur un réseau social et divulgue des informations sensibles. On peut aussi citer le voyageur imprudent qui utilise un réseau wifi public. Les exemples pourraient se multiplier et se décliner dans des variantes infinies. Face à des infrastructures de mieux en mieux sécurisées, les cybercriminels utilisent la vulnérabilité principale d'un système d'information : son utilisateur.

POURQUOI CHERCHER À CROCHETER UNE SERRURE QUAND IL SUFFIT DE TROUVER QUELQU'UN À QUI DEMANDER D'OUVRIR LA PORTE ?

Si, jusqu'à présent, des investissements importants ont été consacrés en cybersécurité, dans la mise en place d'infrastructures, d'analyses de risques, d'équipes spécialisées, le traitement du volet humain de la cybersécurité, lui, fait figure de parent pauvre. Cet aspect, trop longtemps négligé, apparaît aujourd'hui comme stratégique et indispensable. D'un budget quasi inexistant sur le sujet il y a encore 10 ans, les différentes entreprises et organisations publiques ont commencé à accroître leurs moyens dans ce domaine et à planifier des programmes de sensibilisation.
Cependant, il reste encore beaucoup à faire. Un retard s'est accumulé. Il est toujours plus difficile de changer des mauvaises habitudes que de prendre d'emblée les bonnes. L'arrivée d'une nouvelle génération, « digital native », n'arrange rien. En effet, une enquête menée par Pew Research Center en 2018, montre une nettement moindre compréhension de la cybersécurité par les 22-37 ans que par les 54 ans et plus. Par exemple, seuls 58 % des 22-37 ans savent ce qu'est un *phishing* contre 73 % des plus de 54 ans. Les « digital native » seraient-ils aussi des « digital naïve » ?

Disons-le clairement : vous n'obtiendrez pas un niveau de sécurité suffisant sans le renfort des utilisateurs de votre système d'information.

Il est en effet d'usage de pointer du doigt le maillon faible que représente l'utilisateur : « le problème est entre la chaise et le clavier », entend-on souvent. Nous vous proposons ici de renverser ce paradigme. Nous vous proposons de faire de vos utilisateurs le maillon fort de votre cybersécurité. Bien formés, bien entrainés, bien guidés, ils peuvent devenir le meilleur rempart contre les attaques que vous subissez.

Pour atteindre cet objectif, il est indispensable de mettre en œuvre une démarche professionnelle. Comme dans tout domaine il est des choses qui fonctionnent et des choses qui ne fonctionnent pas. L'expérience est riche d'enseignement en la matière. N'oublions pas que l'objectif final est l'instauration d'une véritable culture de la cybersécurité dans votre organisation accompagnée de l'adoption réelle des bons comportements à respecter afin de la protéger.

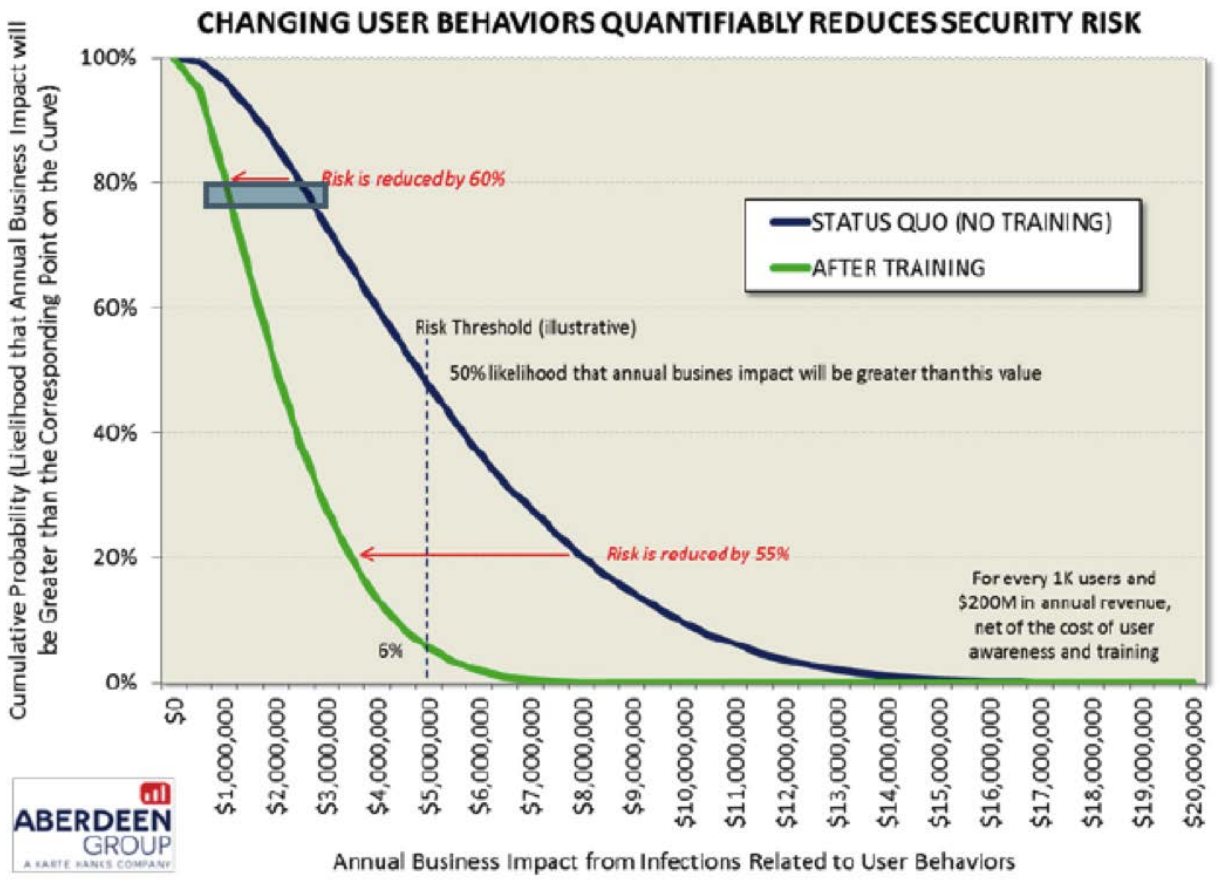
L'objectif de ce *white paper* est de vous présenter une telle démarche, ainsi que certains éléments susceptibles de vous aider dans sa mise en œuvre.

2. POURQUOI SENSIBILISER ?

PARCE QUE ÇA MARCHE.

Il existe peu d'études sur le ROI des opérations de sensibilisation. Le groupe Aberdeen s'est néanmoins attelé à cette tâche en 2014. Le graphique ci-après est extrait de leur étude sur le sujet.

Figure 2: How Changing User Behavior Reduces Security Risk



Source: Aberdeen Group, October 2014

On trouve en abscisses, le coût annuel des incidents de sécurité dus aux comportements des utilisateurs, par tranche de 1 000 utilisateurs et pour 200 millions de dollars de CA. Et, on trouve en ordonnées, la probabilité que le coût des impacts, liés à ces incidents, dépasse la valeur en abscisse. L'étude montre ainsi que la sensibilisation des utilisateurs permet de réduire le coût de ces incidents de sécurité d'environ 60 %. Par exemple, sans sensibilisation, il y a 80 % de chance que l'impact des incidents liés aux comportements des utilisateurs dépasse les 2,5 millions de dollars. Alors, qu'avec un programme de sensibilisation, cette probabilité de 80 % s'applique sur un dépassement de 1,5 million de dollars.

Compte tenu des coûts habituels d'un programme de sensibilisation, on peut affirmer sans crainte que l'investissement dans un tel programme présente le meilleur ROI de tous les investissements consentis en cybersécurité.

PARCE QUE C'EST OBLIGATOIRE.

De nombreuses règlementations, normes et lois demandent à ce que les utilisateurs soient sensibilisés à telle ou telle thématique.
On peut citer notamment :

- RGPD ;
- la réglementation bancaire ;
- PCI DSS ;
- ISO 27001 ;
- LPM ;
- Sapin 2 ;
- loi contre le harcèlement ;
- …

S'il ne devait rester qu'une raison : parce que c'est à l'employeur de donner les consignes.

En effet, cela paraît évident mais cela a longtemps été ignoré en ce qui concerne les bons comportements à adopter en matière de cybersécurité : c'est à l'employeur de donner les consignes et d'expliquer ce qui est attendu de la part des collaborateurs.
Cela conduit à l'élaboration de charte qu'il convient ensuite d'expliquer. La sensibilisation est la traduction des consignes de l'entreprise ou de l'organisation en matière de comportement attendus, acceptés, tolérés et interdits quant à l'usage du système d'information.

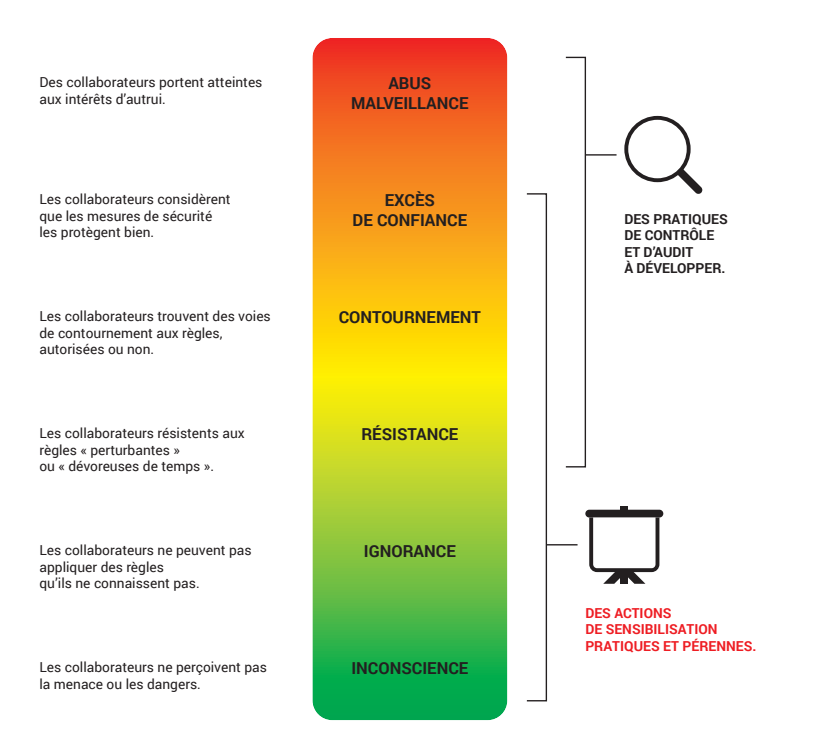
On évite ainsi l'excuse facile : « Ah mais je ne savais pas ».

3. LA DÉMARCHE

LA SENSIBILISATION N'EST PAS UN PROJET, C'EST UN PROCESSUS.

3.1 INTÉGRER LE FACTEUR HUMAIN AU BON NIVEAU

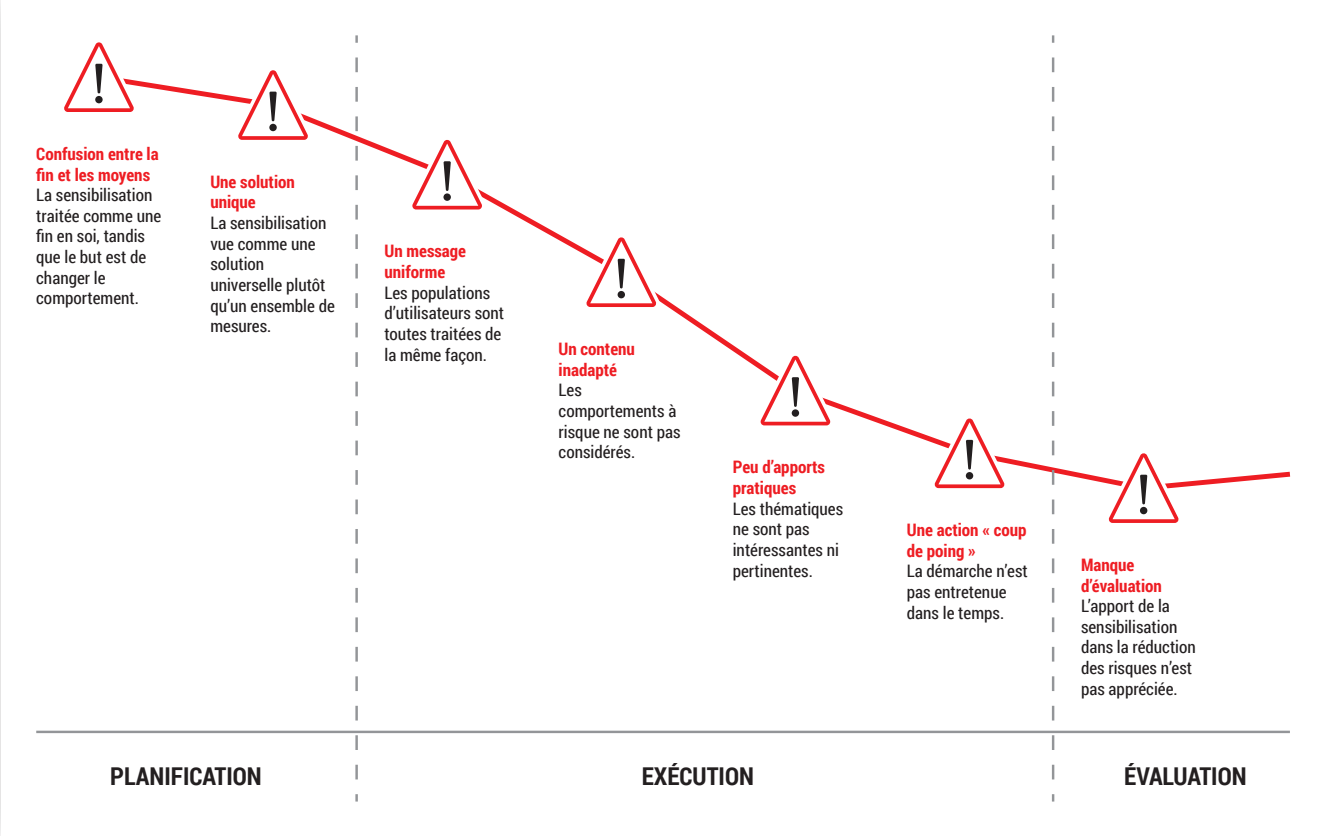
Les défauts des utilisateurs les conduisant à un mauvais comportement en cybersécurité sont au nombre de 6 : l'inconscience, l'ignorance, la résistance, le contournement, l'excès de confiance et la malveillance.
La correction de chaque défaut n'appelle pas la même réponse qui doit s'adapter à ce contre quoi elle lutte.
Ainsi la sensibilisation s'attachera aux 5 premiers niveaux :



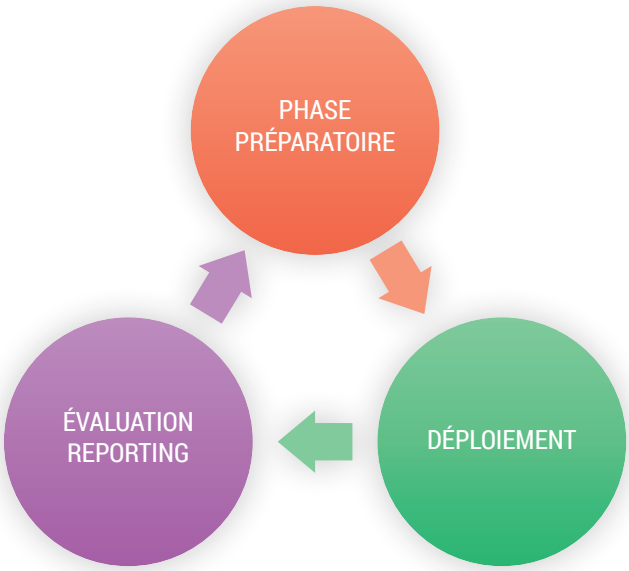
La définition d'une stratégie de sensibilisation tient donc compte de ces différents défauts et fait en sorte de répondre à chacun d'entre eux.

Il convient également de garder en mémoire les 7 erreurs les plus courantes, à éviter pour obtenir l'efficacité maximale de cette stratégie. On peut résumer des 7 erreurs ainsi :

LES 7 ERREURS À NE PAS COMMETTRE

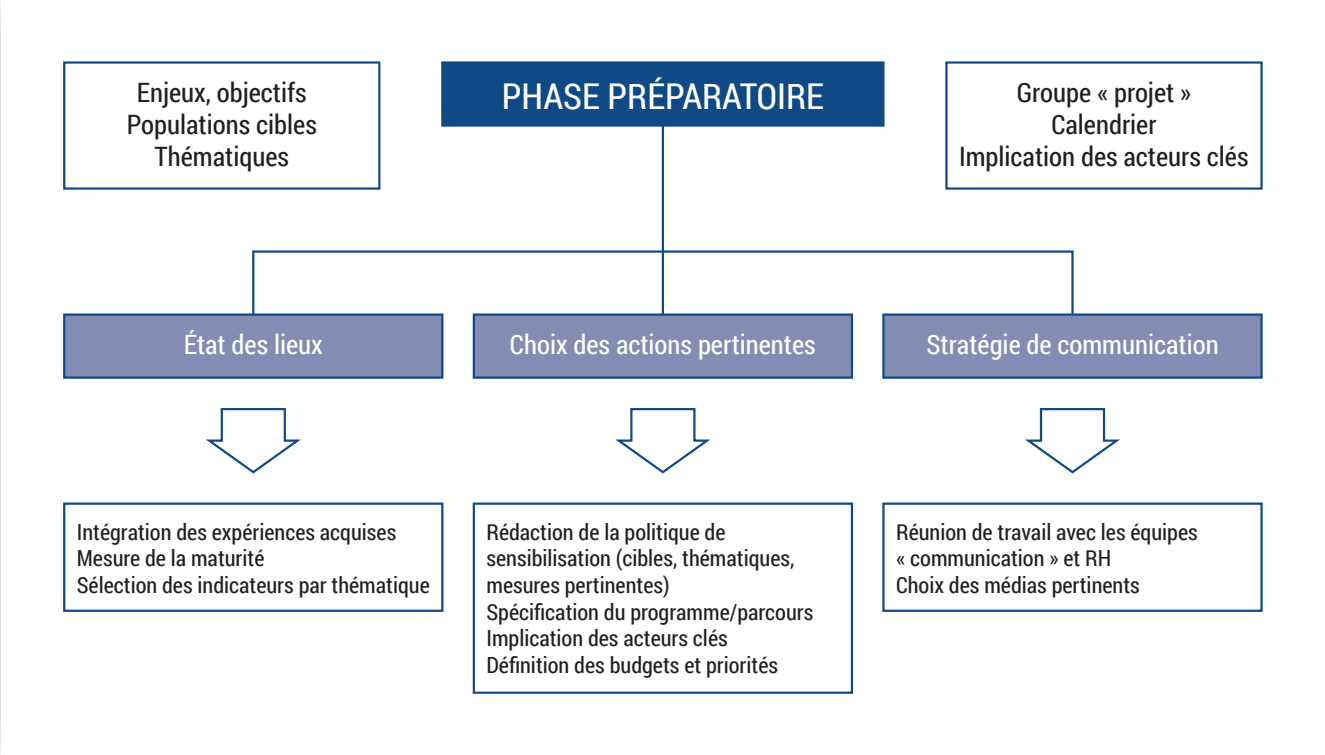


La mise en œuvre d'une stratégie de sensibilisation n'étant pas un projet mais un processus, elle s'appuie sur un cycle sans cesse répété incluant 3 étapes :



3.2 PHASE PRÉPARATOIRE

La phase préparatoire peut se résumer par le graphique suivant.



Cette phase est essentielle. De sa qualité dépend l'efficacité des actions qui seront menées. En fonction de la maturité de l'organisation, cette phase sera plus ou moins conséquente. En effet, selon que l'on prépare la première opération de sensibilisation ou que l'on soit dans le cadre d'une mise à jour réalisée à l'issue d'un cycle du processus de sensibilisation, le travail à fournir ne sera pas le même.

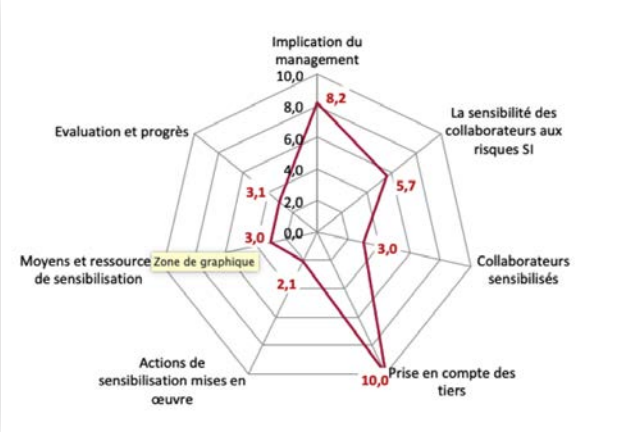
FAIRE UN ÉTAT DES LIEUX

Un état des lieux va permettre de savoir d'où l'on part. Il permettra également de mettre en œuvre les outils de mesures qui permettront, dans le temps, de mesurer le chemin parcouru et de définir des objectifs.

Parmi les outils utilisables pour effectuer l'état des lieux on peut notamment citer :

- le questionnaire d'auto-évaluation de la maturité, destiné au management ;
- ISAM (Information Security Awareness Meter) à destination de tous ;
- les campagnes de *phishing* factices.

L'auto-évaluation à destination du management s'appuie sur un questionnaire structuré en 7 thèmes.

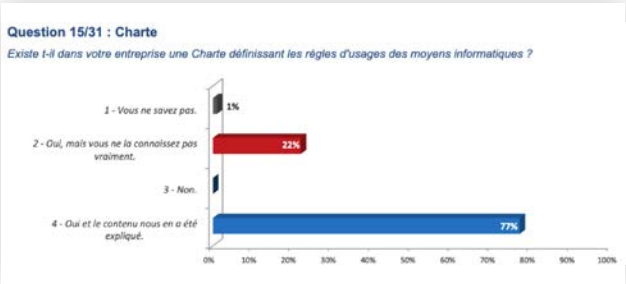


Le RSSI et quelques managers répondent à ce questionnaire. Les résultats collectés et agglomérés permettent d'établir une grille de lecture de la maturité de l'organisation.

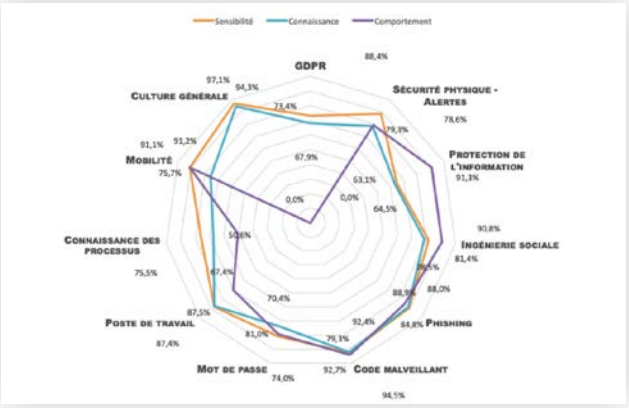
Critères du questionnaire	Points obtenus	Commentaires
Implication du management	**8,2/10**	Le management est **fortement impliqué** dans les relations avec les équipes SI et les problématiques liées à la sécurité des SI et protection des informations.
La sensibilité des collaborateurs aux risques SI	**5,7/10**	Les collaborateurs sont plutôt actifs et sensibles sur tout ce qui concerne les remontées d'incidents et l'application des bonnes pratiques pour la sécurité des systèmes d'information et protection des informations.
Collaborateurs sensibilisés	**3,0/10**	Les collaborateurs sont très **peu sensibilisés** par profil spécifique (dirigeants, administrateurs, etc.) sur la sécurité des SI et la protection des informations.
Prise en compte des tiers	**10/10**	Avec une note maximum, les tiers sont très bien suivis sur les sujets de sécurité des SI de leur entrée à leur sortie de la société.
Actions de sensibilisation mises en œuvre	**2,1/10**	Pas ou peu de sensibilisation menées jusqu'à présent. En revanche, le management et le RSSI ont conscience de la nécessité de déployer les actions correspondantes.
Moyens et ressources de sensibilisation	**3,0/10**	Pas de moyens et ressources de sensibilisation utilisés à ce jour. Ces derniers sont prévus mais restent à déployer et à mettre en œuvre (objectif de la prestation en cours).
Évaluation et progrès	**3,1/10**	Une évaluation des connaissances de base est à réaliser, ainsi que des tests formels en interne pour faire prendre conscience des risques et des bonnes pratiques à associer.

L'outil ISAM (Information Security Awareness Meter) a été mis au point par Conscio Technologies. Il consiste en une enquête dont la version 2019 comporte 25 questions qui est adressé sous forme d'un quiz *e-learning* à l'ensemble des collaborateurs. ISAM permet une évaluation sur 3 niveaux.

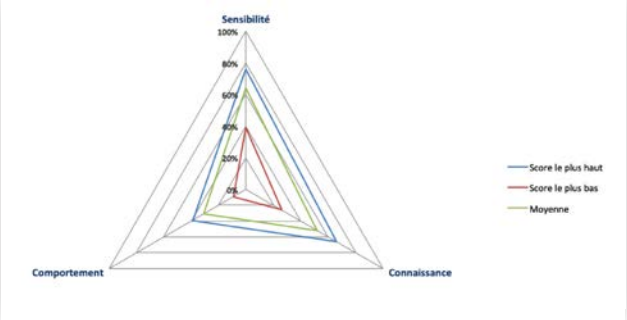
Analyse de certaines questions clés individuellement.
Exemple :



Analyse par thématique.
Exemple :



Analyse sur les 3 axes : sensibilité, connaissances et comportements



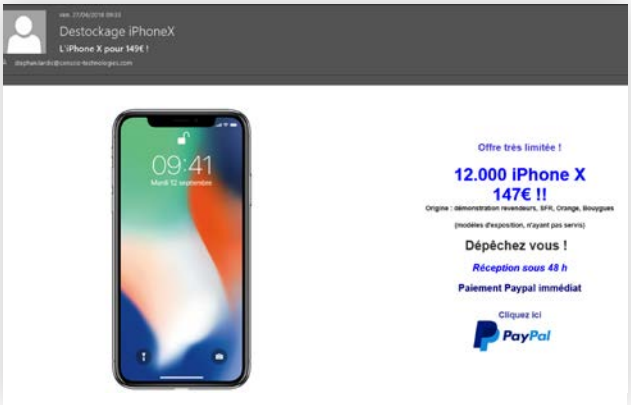
Un outil comme ISAM permet de consulter tous les collaborateurs et de disposer d'un véritable outil de mesure, au plus près du terrain, de leur niveau de maturité. Il est ainsi facile de dégager les actions à mener, de communiquer auprès d'un comité de direction et de mesurer le chemin parcouru ensuite par une nouvelle enquête.

FAIRE DES PHISHING FACTICES

Les campagnes de *phishing* factices permettent de tester la résilience d'une population face aux tentatives de *phishing*.

Le *phishing* est le vecteur numéro 1 d'introduction d'un code malveillant ou d'une cyberattaque. On peut donc, en complément d'une sensibilisation didactique en la matière, tester le comportement réel des utilisateurs face à cette menace au moyen de *phishing* factices.

Il faut varier les approches, les scénarios, s'adapter aux cultures locales et mener ces opérations régulièrement.
Exemple :



Cela permet d'obtenir une mesure supplémentaire, d'en voir l'évolution et de définir des objectifs.
Il faut cependant faire attention au biais de ce genre d'opérations. En effet, par exemple, si une personne ne clique pas, cela ne veut pas dire qu'elle est forcément vigilante : elle n'a peut-être pas vu le message ou, tout simplement, le sujet abordé ne l'intéresse pas.

STRATÉGIE DE SENSIBILISATION

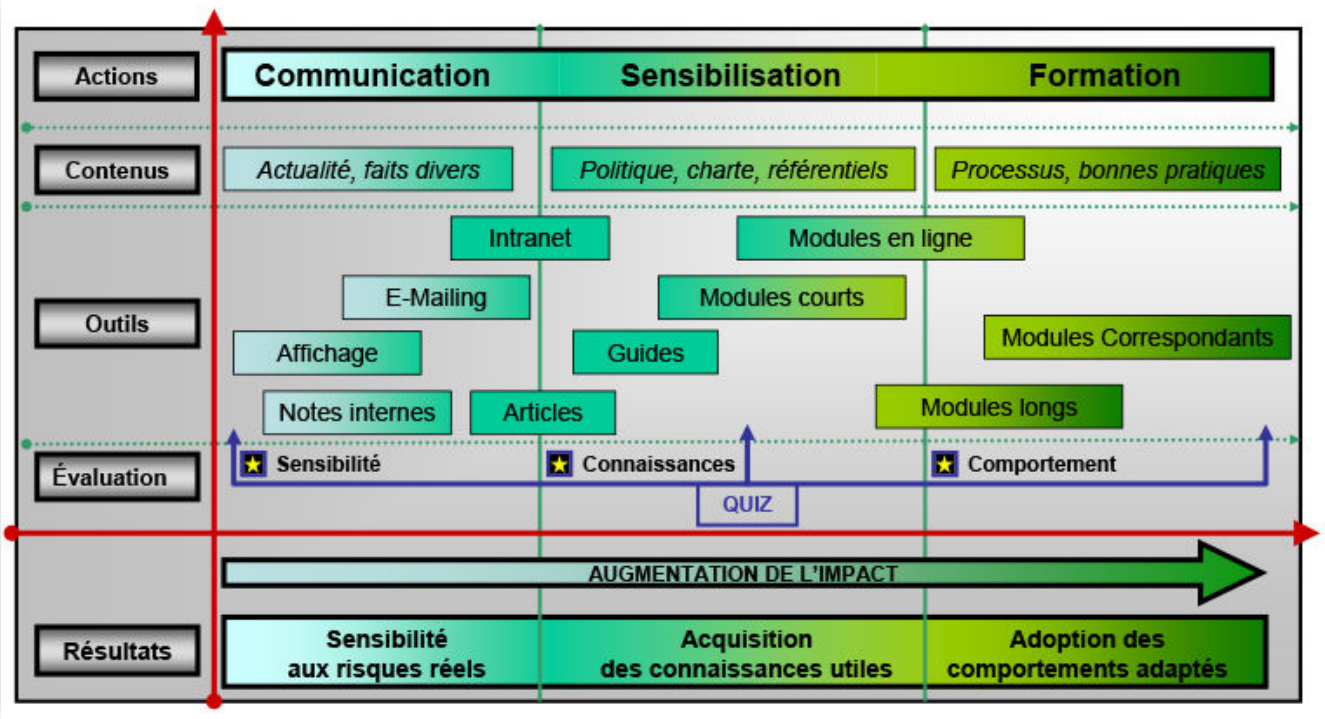
Une stratégie de sensibilisation s'apparente à une stratégie de communication. Il faudra en effet s'attacher à identifier le QUI, choisir le QUOI en fonction du QUI, puis le COMMENT, et placer le tout dans la durée, QUAND.
Classiquement parmi le « QUI ? » on peut retrouver les catégories de population suivantes :

- **les décideurs et managers** :
  impulsion et exemplarité :
  - soutien de la démarche de sensibilisation,
  - responsabilité légale,
  - règles spécifiques (données stratégiques, mobilité…) ;
- **l'ensemble des collaborateurs** :
  positiver la sécurité :
  - salarié/citoyen/consommateur,
  - engagement, implication, éthique,
  - responsabilité légale ;
- **les profils spécifiques** :
  - assistantes,
  - nomades,
  - etc. ;
- **les informaticiens** :
  - fonctions « projets »,
  - fonctions « développeurs »,
  - fonctions « opérations »,
  - fonctions « help desk/service desk »,
  - fonctions « support » ;
- **les correspondants/relais** : les clés de la culture :
  - compréhension de la politique et de l'organisation,
  - capacité à répondre aux questions des collaborateurs ;
- **les tiers** :
  - consultants,
  - sous-traitants,
  - clients.

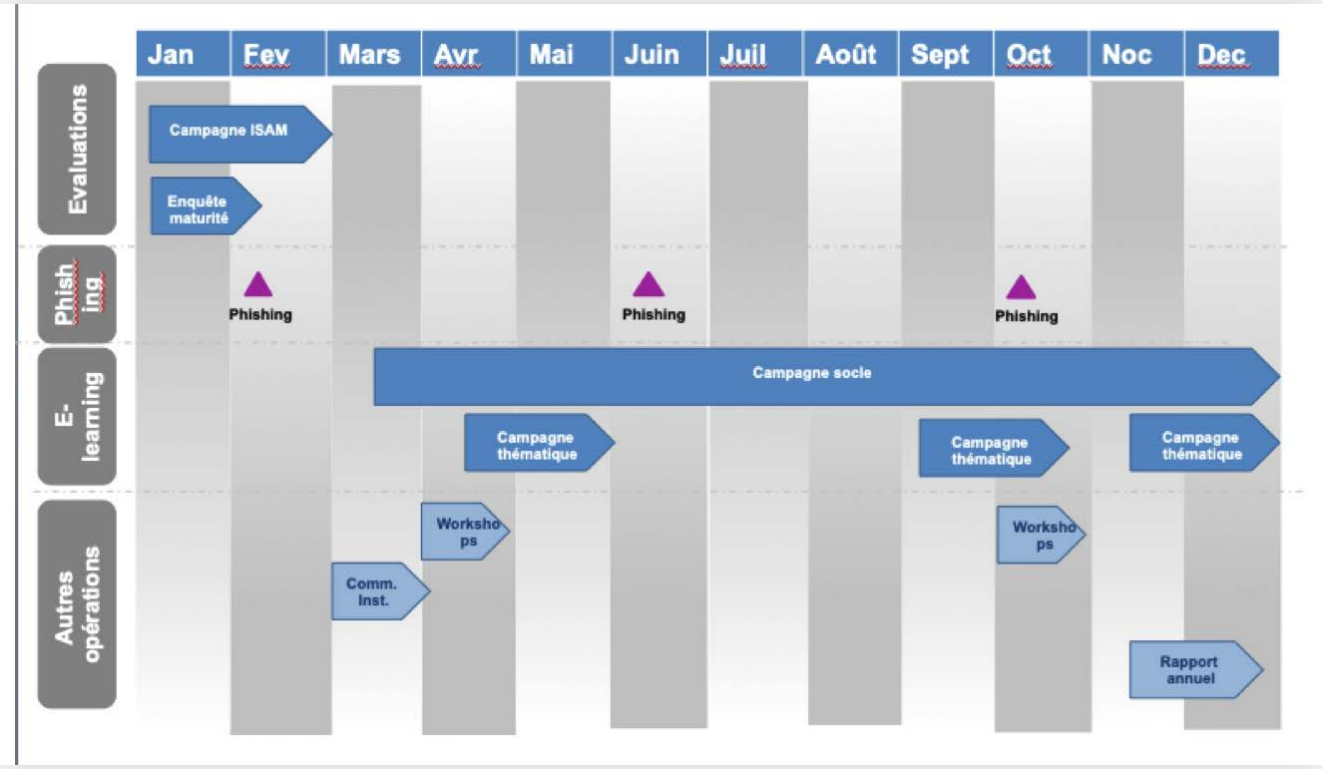
Le « QUOI ?» dépendra du « QUI ? » mais également de ce qui aura déjà été fait, des faiblesses identifiées, de l'actualité, des principales menaces, etc.
Classiquement on retrouve :

- « **les incontournables** » :
  - protection de l'information,
  - *phishing*,
  - navigation sûre,
  - codes malveillants,
  - ingénierie sociale,
  - mots de passe,
  - poste de travail,
  - supports amovibles,
  - accès physiques ;
- « **les spécifiques** » :
  - mobilité,
  - données clients,
  - informatique et libertés/RGPD,
  - données stratégiques/intelligence économique,
  - aspects légaux/responsabilités,
  - continuité d'activité/gestion de crise,
  - contenus informaticiens ;
- « **à la maison** » :
  - travailler sur son PC personnel,
  - protéger son PC,
  - protéger les enfants,
  - acheter en ligne.

Les actions liées au « COMMENT ? » sont également multiples. Elles dépendront des budgets disponibles, des habitudes de l'organisation, de la capacité à mobiliser les acteurs, etc.
Le graphique suivant regroupe un certain nombre d'actions possibles.



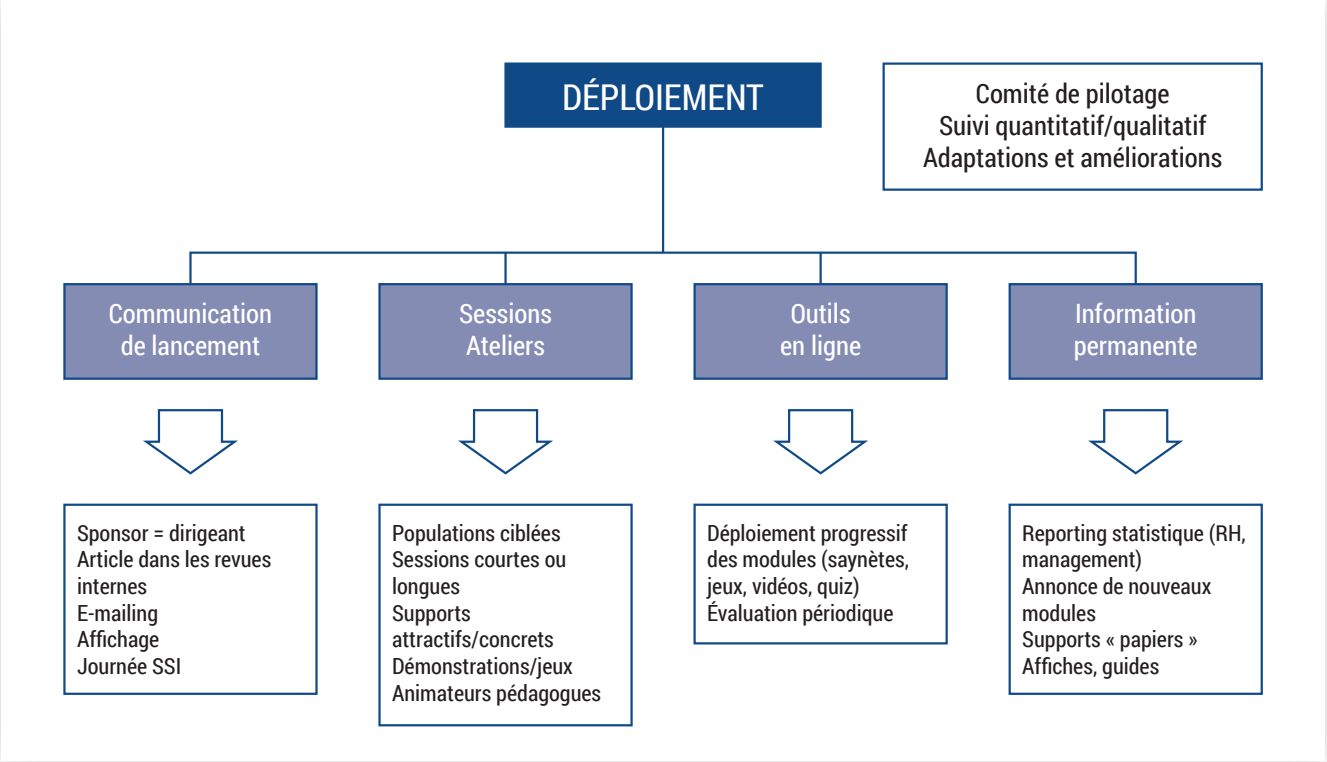
L'ensemble des ces actions seront ensuite organisés dans le temps sur un planning de sensibilisation, reprenant la stratégie dans son ensemble.
Exemple :



3.3 DÉPLOIEMENT

Le graphique ci-après regroupe les principales actions de déploiement.

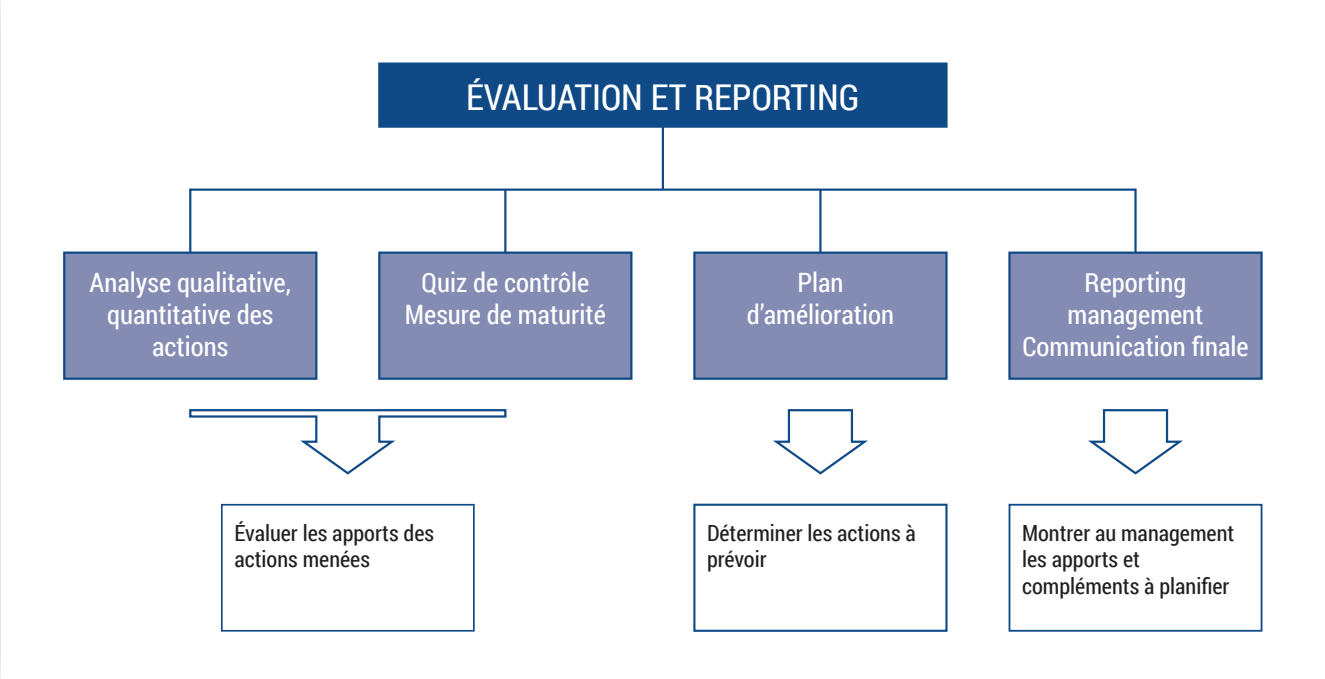
Il s'agit de mettre en œuvre la stratégie préalablement définie. On s'attachera tout le long du déploiement au suivi de certains indicateurs clés : taux de participation, taux de complétude, notamment. En fonction de ces indicateurs on renforcera les opérations de communications, de relances, d'actions des sponsors.



3.4 ÉVALUATION ET REPORTING

Indispensable pour s'inscrire dans un processus d'amélioration continue et de développement d'une culture cybersécurité, chaque action devra faire l'objet d'une évaluation.

De cette façon, on repassera après dans une nouvelle phase de préparation des opérations suivantes.



4. LES 10 FACTEURS CLÉS DE SUCCÈS

Issus d'une expérience acquise sur plus de 200 projets auxquels nous avons participé sur les 12 dernières années, nous avons regroupé ici les 10 facteurs clés de succès d'une opération de sensibilisation en ligne.

4.1 FACTEUR CLÉ DE SUCCÈS N° 1 : AVOIR UNE MESURE

Dans une optique de développement de la culture cyber il est particulièrement important de se doter d'une mesure. En effet celle-ci permet de :

- faire un état des lieux du niveau de maturité des collaborateurs ;
- définir un objectif de progression ;
- mesurer le chemin parcouru ;
- inscrire dans une démarche d'amélioration permanente ;
- pouvoir communiquer sur les résultats et justifier les investissements nécessaires.

Pour établir cette mesure on peut se baser sur différents indicateurs et statistiques :

- les réponses faites au quiz lors de campagnes de sensibilisation en ligne. Ces réponses viennent alimenter des statistiques que l'on peut agréger selon les thématiques traitées et selon les différentes caractéristiques utilisateurs. Il est aussi possible de définir un seuil de validation de la campagne et ainsi avoir un indicateur sur le taux de personnes ayant validé une campagne ;
- les résultats d'une enquête telle qu'ISAM, dont on a déjà parlé plus haut. ISAM permet l'évaluation de la maturité d'une population au regard de la cybersécurité. Cette évaluation est faite sur 3 niveaux :
  - par question,
  - par thématique,
  - selon les 3 axes : sensibilité, connaissances et comportements. Avec ISAM il est également possible de se « benchmarker » et donc de se situer par rapport à un panel d'entreprises ;
- les résultats d'une campagne de *phishing* factice. Même s'il faut relativiser la mesure faite par ce type de campagne, certaines personnes ne cliquent pas sur le message non pas parce qu'elles sont vigilantes mais simplement parce qu'elles ne voient pas le message ou parce que le sujet abordé ne les concerne pas, son évolution dans le temps dénotent d'une meilleure sensibilisation au risque de *phishing* ;
- audit et tests pouvant couvrir :
  - tests de résistance sur les mots de passe,
  - audit des bureaux pour les verrouillages de postes de travail,
  - pentests d'ingénierie sociale.

Cette série d'indicateurs permet de se constituer un véritable tableau de bord de la sensibilisation qui peut ainsi venir compléter un tableau de bord de la sécurité.

4.2 FACTEUR CLÉ DE SUCCÈS N° 2 : AVOIR UN SPONSOR À LA DIRECTION

Notre expérience sur près de 200 projets de sensibilisation en ligne fait apparaître des taux de participation qui vont de 10 % à 80 % environ, dans le cadre de campagnes non obligatoires. La moyenne se situe en général entre 55 % et 65 %. Ce qui, bien souvent, fait la différence entre une bonne et une mauvaise participation, est le niveau d'engagement de la Direction.

Le développement de la maturité d'une population sur la cybersécurité passe tout d'abord par un bon niveau de sensibilité au sujet. Dès lors comment être sensible à ce sujet dans son entreprise si l'on ne sent pas qu'il s'agit d'une préoccupation des dirigeants ? L'exemple a ici force d'adhésion. Impossible en effet de prendre le sujet au sérieux si les premiers contrevenants aux bonnes pratiques se trouvent au sommet de la pyramide. Il est donc souhaitable d'associer, à l'annonce de votre campagne de sensibilisation, un message de la Direction. Celui-ci peut prendre diverses formes :

- l'extrait d'une communication officielle incluse dans le mail d'invitation à la campagne ;
- une courte vidéo en introduction de la campagne ;
- l'annonce de la campagne faite directement par la Direction.

Fin 2019, la plupart des dirigeants sont conscients des risques que fait peser la cybercriminalité sur l'activité de leur organisation. Nombre d'entre eux ont également compris qu'une bonne stratégie de cybersécurité s'appuie sur une organisation, de la technologie et sur un volet humain d'autant plus important que la majorité des cyberattaques réussies passe par une défaillance humaine.

Si vous avez cependant besoin de sensibiliser votre Direction sur l'importance des enjeux vous pouvez :

- mettre en avant la règlementation. À ce titre le RGPD précise les obligations à respecter en matière de protections des données et renforce considérablement les sanctions. Celles-ci ne peuvent notamment plus être ignorées par les Directions des entreprises ;
- rendre tangible le risque encouru en prenant appui sur des piratages déjà survenus dont on parle de plus en plus dans les médias ou, le cas échéant, déjà survenus au sein de votre organisation ;
- mettre en avant les bonnes pratiques en cybersécurité ;
- mettre en avant un état des lieux de la maturité des collaborateurs au regard de la cybersécurité. Établissement d'une mesure et définition d'objectifs chiffrés. Faire exister la sensibilisation auprès des Directions passe aussi par la mise en place d'indicateurs et d'objectifs clairs en face desquels on peut demander un budget. C'est pour cette raison que la définition d'une mesure a été placée comme facteur clé de succès n° 1.

4.3 FACTEUR CLÉ DE SUCCÈS N° 3 : AVOIR UNE STRATÉGIE PLANIFIÉE

Faire progresser une culture cybersécurité est une tâche à la fois longue et ardue. Même s'il est maintenant reconnu que les actions de sensibilisation à la cybersécurité offrent le ROI le plus élevé parmi l'ensemble des projets de sécurité à mener, seule la définition d'une stratégie claire et planifiée permet de rentabiliser au mieux ses efforts de sensibilisation.
La démarche de sensibilisation s'apparentant à une opération de communication, il est indispensable de répondre aux questions suivantes :

QUI ?

À qui s'adresse la sensibilisation ?
Vais-je faire une sensibilisation commune à tout le monde ?
Est-ce que j'ajoute des contenus spécifiques en fonction des métiers ?
Comment j'adresse la Direction, le management ?
Quelle sensibilisation pour les nouveaux arrivants, les personnes qui ne sont pas équipés de PC ? …

QUOI ?

Quels sont les sujets à aborder ?
Les essentiels ?
Des sujets métiers spécifiques ? RGPD ? …

COMMENT ?

Sous quel format la sensibilisation va t'elle se dérouler : *workshop*, séances plénières, présentiel, *e-learning*, e-mails, livrets, *goodies* ?…

QUAND ?

Il s'agit ensuite de cadencer l'ensemble des opérations dans le temps.
La combinaison de l'ensemble de ces éléments permet de définir sa stratégie de sensibilisation avec un plan d'actions clair et cadencé. Ce document permet ainsi de communiquer sur sa stratégie et donc de se coordonner avec les autres services impliqués : Ressources humaines, Communication…
Il faut enfin inscrire la stratégie dans le cadre d'une démarche permanente d'amélioration continue. Les résultats de toutes les opérations doivent être mesurés et ainsi permettre de définir des objectifs et de mesurer le chemin parcouru.

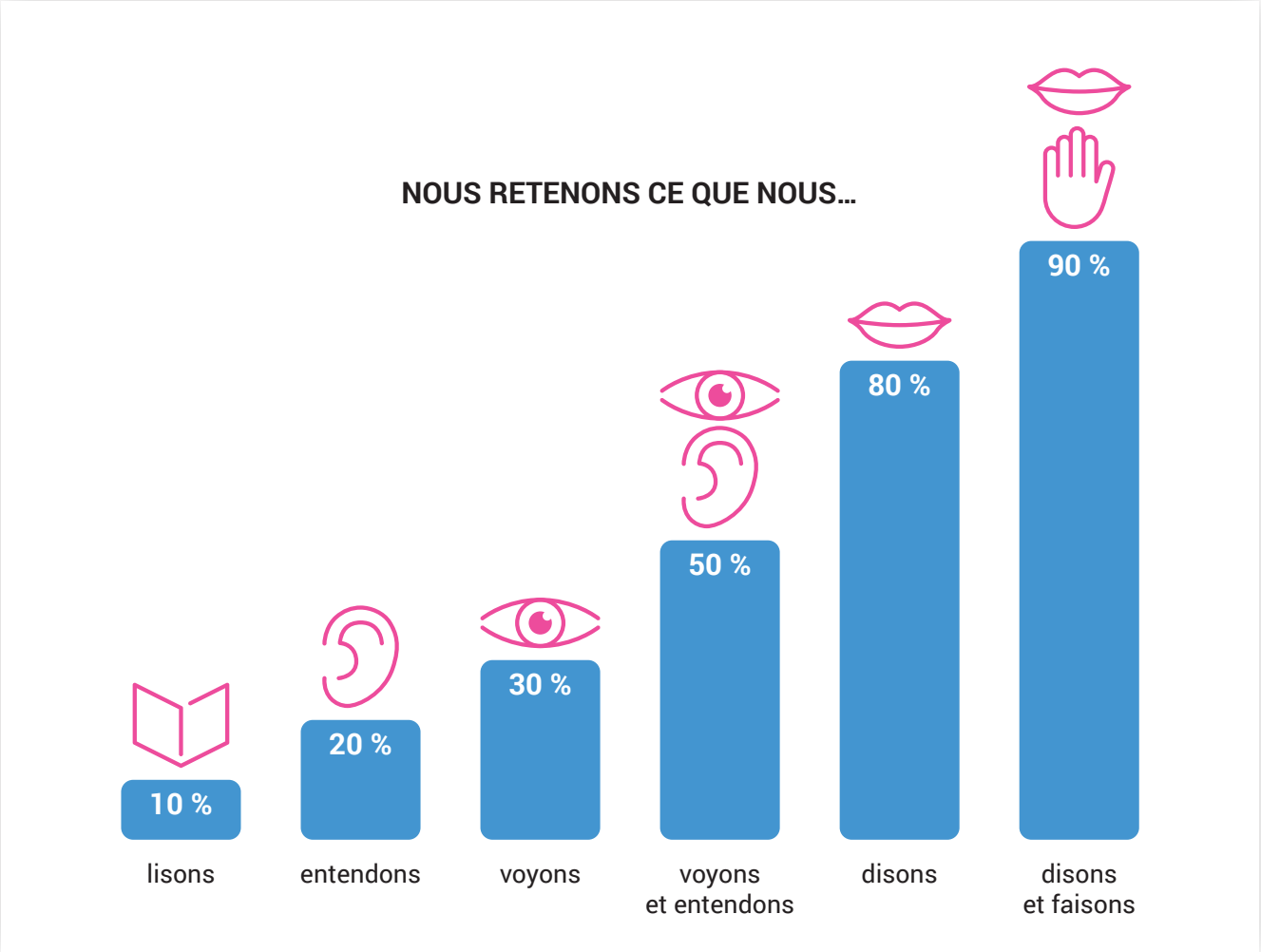
4.4 FACTEUR CLÉ DE SUCCÈS N° 4 : DONNER ENVIE

Une opération de sensibilisation se trouve à la frontière entre une opération de formation et une opération de communication.
En effet, nombre d'entreprises incluent les parcours de sensibilisation en ligne dans la catégorie *e-learning*. Ces contenus sont intégrés dans le parcours de formation des personnes et leur réalisation est suivie comme telle dans leur décompte de formation. La formation ainsi apportée est mesurée en temps passé avec une liste de sujets abordés (risques cybersécurité, bonnes pratiques à respecter, connaissances cybersécurité de base…).
La fourniture de contenus ou l'utilisation de plates-formes de sensibilisation peuvent ainsi donner lieu à la mise en place de conventions de formation.
La sensibilisation, cependant, diffère par certains aspects de la plupart des formations. En effet, dans le cadre d'une formation, l'apprenant est en général motivé par ce que la formation va lui apporter en termes d'évolution personnelle et professionnelle. Cette motivation est très peu présente dans le cadre d'une campagne de sensibilisation. Même si le sujet de la cybersécurité suscite un intérêt indéniable, la prise en compte des mesures de sécurité est encore très souvent vécue comme une contrainte. En ce sens, il est indispensable de donner envie, si l'on veut obtenir la participation la plus large.
Pour donner envie, le contenu proposé devra :

- être attractif avec un design plaisant et agréable ;
- être facile d'accès et d'emploi ;
- ne pas provoquer de situation d'échec, afin d'éviter le rejet de la campagne par l'apprenant ;
- coller au maximum aux situations vécues par l'apprenant ;
- dans certains cas, être renforcé par l'obtention de récompense ou de reconnaissance : certificats ou, éventuellement, remises de *goodies*.

4.5 FACTEUR CLÉ DE SUCCÈS N° 5 : UNE COMMUNICATION ENGAGEANTE

La pyramide de l'apprentissage est claire. Plus on participe et plus on agit lors de la formation et meilleure sera la rétention de son contenu.



Il faut donc que le contenu proposé soit le plus interactif possible. Sans sacrifier à la simplicité d'accès et d'usage, il faut pouvoir amener l'utilisateur à suivre les scénarios proposés et avoir la possibilité d'interagir avec eux. Derrière ce constat de bon sens, se profile la notion de communication engageante.

Je reprends ici un extrait d'un livre blanc sur la sensibilisation que nous avions rédigé il y a quelques années et qui garde encore sa pertinence.

COMMENT AGIR EFFICACEMENT SUR LES COMPORTEMENTS ?

Depuis soixante ans maintenant les chercheurs en sciences humaines et sociales (en particulier les chercheurs en psychologie sociale) s'intéressent à cette question.

LEURS RECHERCHES MONTRENT D'ABORD LES LIMITES DE L'AUTORITÉ.

L'ombre du bâton disparu, chacun retrouve peu ou prou ses mauvaises habitudes. Cela peut facilement se comprendre. Si dans une organisation donnée un collaborateur se comporte dans telle ou telle situation comme un agent de pouvoir l'exige, il peut éviter d'en appeler à ses valeurs ou à ses propres motivations pour expliquer ce qu'il fait, car il dispose d'une raison « externe » toute prête : éviter une punition. C'est la raison pour laquelle les changements obtenus autoritairement ne sont pas durables. Si, en matière de sécurité, l'autorité est évidemment nécessaire, elle n'est en aucun cas suffisante.

LES RECHERCHES MONTRENT ENSUITE LES LIMITES DE L'INFORMATION ET DE LA PERSUASION.

Pourtant, l'information et la persuasion peuvent s'avérer très efficaces pour modifier les idées que quelqu'un peut avoir sur telle ou telle question. Malheureusement, il ne suffit pas d'avoir les « bonnes idées » pour avoir les « bons comportements ».
Il ressort d'une très sérieuse étude longitudinale réalisée il y a quelques années aux États-Unis que la probabilité d'être fumeur à 17 ans n'est pas plus faible chez des élèves ayant pourtant suivi pas moins de 65 séances de « sensibilisation » entre 8 ans et 17 ans (condition expérimentale) – et donc parfaitement informés des méfaits du tabac – que chez des élèves n'ayant pas suivi ces séances (condition contrôle). Et cette étude n'est qu'une des très nombreuses recherches qui illustrent le décalage qu'il peut y avoir entre nos idées – en l'occurrence nos « bonnes idées » – et nos actes. Évidemment, cela ne signifie pas qu'informer ne sert à rien ou qu'argumenter ne sert à rien. L'information et l'argumentation servent incontestablement au fil du temps à modifier les savoirs, les idées, les attitudes et même, certainement, à provoquer de réelles prises de conscience. Il reste que, pas plus que l'autorité, elles ne sont suffisantes.

Heureusement les recherches montrent aussi qu'il suffit parfois de peu de chose pour passer des idées aux actes. Et les chercheurs n'ont pas manqué de faire de ce peu de chose un objet d'étude privilégié, si bien qu'on dispose aujourd'hui de tout un savoir scientifique sur lequel on peut s'appuyer pour gagner en efficacité. Robert-Vincent Joule et Jean-Léon Beauvois, deux chercheurs français réputés et auteurs de nombreux ouvrages, ont contribué à faire avancer les connaissances sur cette question. Dans leur ouvrage de référence, ils font état d'une bonne dizaine de techniques sur lesquelles on peut tabler pour aider autrui à modifier librement ses comportements (cf. Joule et Beauvois, 2002, Joule, *Petit traité de manipulation à l'usage des honnêtes gens*. Grenoble : Presses Universitaires de Grenoble). Ces techniques passent pour la plupart par l'obtention d'un petit comportement, très facile à obtenir tant il est peu coûteux, mais qui va prédisposer celles et ceux qui l'ont réalisé à en réaliser d'autres, par la suite, bien plus coûteux. La dynamique de changement est ainsi enclenchée. C'est la raison pour laquelle ces petits comportements, qui sont à la base même du processus de changement sont appelés : « comportements préparatoires ».

L'intérêt de ces techniques est de conduire à la responsabilisation des acteurs qui en arrivent à prendre librement les engagements que l'on attend d'eux, à les assumer, et à intérioriser les traits ou les valeurs qui vont assurer la pérennité de leurs nouvelles conduites. C'est dire l'intérêt de ces techniques dont l'efficacité est démontrée dans de nombreux domaines de la vie sociale (cf. notamment, Joule et Beauvois, 1998, *La soumission librement consentie*. Paris : Presses Universitaires de France).

La notion d'engagement est ici centrale. Un extrait d'un texte de Robert-Vincent Joule va nous aider à mieux appréhender cette notion.

LA PSYCHOLOGIE DE L'ENGAGEMENT

C'est dans la psychologie de l'engagement qu'il convient de rechercher l'assise théorique sur laquelle reposent les principales techniques permettant d'obtenir sans imposer.
Gardons en mémoire que c'est la situation qui, en fonction de ses caractéristiques objectives, engage ou qui n'engage pas l'individu dans ses actes.

DÉFINITIONS DE L'ENGAGEMENT

« L'engagement correspond, dans une situation donnée, aux conditions dans lesquelles la réalisation d'un acte ne peut être imputable qu'à celui qui l'a réalisé. » (Joule et Beauvois, 1998, p. 60)

LES EFFETS DE L'ENGAGEMENT

- Sur le plan cognitif, l'engagement débouche sur une consolidation des attitudes, et sur une plus grande résistance au changement (effet de gel), il peut même déboucher sur un meilleur ajustement de l'attitude à l'acte réalisé (effet de rationalisation).
- Sur le plan comportemental, l'engagement débouche sur une stabilisation du comportement et sur la réalisation de nouveaux comportements allant dans le même sens.

Aussi, la psychologie de l'engagement propose-t-elle un éclairage théorique différent de certains processus psychologiques (appropriation, rationalisation, ou au contraire rejet, extrêmisation, etc.) en jeu dans les organisations, processus susceptibles de favoriser le changement ou, au contraire de le freiner.

COMMENT OBTENIR UN FORT ENGAGEMENT ?

On peut obtenir un fort engagement en jouant sur plusieurs facteurs, dont les principaux sont :

- le contexte de liberté dans lequel l'acte est réalisé : un acte réalisé dans un contexte de liberté est plus engageant qu'un acte réalisé dans un contexte de contrainte ;
- le caractère public de l'acte : un acte réalisé publiquement est plus engageant qu'un acte dont l'anonymat est garanti ;
- le caractère explicite de l'acte : un acte explicite est plus engageant qu'un acte ambigu ;
- l'irrévocabilité de l'acte : un acte irrévocable est plus engageant qu'un acte qui ne l'est pas ;
- la répétition de l'acte : un acte que l'on répète est plus engageant qu'un acte qu'on ne réalise qu'une fois ;
- les conséquences de l'acte : un acte est d'autant plus engageant qu'il est lourd de conséquences ;
- le coût de l'acte : un acte est d'autant plus engageant qu'il est coûteux (en argent, en temps, en énergie, etc.) ;
- les raisons de l'acte : un acte est d'autant plus engageant qu'il ne peut être imputé à des raisons externes (par exemple : promesses de récompenses, menaces de punition) et qu'il peut être imputé à des raisons internes (par exemple : valeurs personnelles, traits de personnalité).

4.6 FACTEUR CLÉ DE SUCCÈS N° 6 : FAIRE SIMPLE ET ACCESSIBLE

Votre campagne de sensibilisation va s'adresser à priori à une population très hétérogène. Dans votre entreprise ou votre organisation, travaillent probablement des femmes et des hommes d'âges, de sensibilités, de métiers, de compétences et de cultures différents.

VOTRE SENSIBILISATION DOIT POUVOIR LES TOUCHER TOUS.

Pour ce faire vous pouvez utiliser plusieurs canaux de diffusion et plusieurs types d'outils.
Il n'en reste pas moins que quelques soient ces derniers, il est indispensable de faire simple et accessible.
Les collaborateurs, aujourd'hui sollicités de toute part, avec un emploi du temps contraint, doivent pouvoir accéder à votre contenu directement, simplement, sans se poser de questions.
C'est pourquoi tout support nécessitant la moindre réflexion de prise en main ou ne rentrant pas directement dans le vif du sujet est à éviter. Si le collaborateur doit réfléchir ou rechercher comment faire fonctionner le contenu proposé, c'est autant de temps pris sur son temps disponible pour suivre la sensibilisation et autant de risques qu'il laisse tomber et passe à autre chose.

Lorsque vous invitez les collaborateurs à suivre une campagne en ligne, il est préférable de leur en permettre l'accès en un seul clic.
Le contenu doit ensuite pouvoir se dérouler simplement de façon familière au regard de ce à quoi est habitué le collaborateur.

À cet égard les capsules de type micro Learning constituées d'une courte vidéo suivie de deux à trois QCM, sont à l'heure actuelle, une solution particulièrement adaptée.
Cela peut bien sûr être différent en fonction de ce à quoi votre population est habituée.

L'essentiel est de faire simple, de se mettre à leur place et de comprendre combien le temps qu'ils vont allouer à votre campagne est précieux.

4.7 FACTEUR CLÉ DE SUCCÈS N° 7 : PROCÉDER PAR TOUCHES SUCCESSIVES

L'objectif de la sensibilisation est le développement d'une réelle culture cybersécurité et l'adoption des bons comportements de nature à protéger le système d'information. Réaliser une grosse campagne annuelle, si elle permet de remplir ses obligations règlementaires, n'est pas forcément le meilleur moyen pour y parvenir.

Afin de rester présent dans les esprits et favoriser l'ancrage d'une telle culture, il vaut mieux pouvoir mettre en œuvre plusieurs rendez-vous cybersécurité dans l'année. Et, la seule façon réaliste de les réaliser est de faire court à chaque fois.

À LA MANIÈRE D'UN PEINTRE IMPRESSIONNISTE, IL FAUT AINSI PROCÉDER PAR TOUCHES SUCCESSIVES.

4.8 FACTEUR CLÉ DE SUCCÈS N° 8 : UN DÉPLOIEMENT AISÉ

En fonction de la taille de votre organisation, vos campagnes vont devoir cibler plusieurs centaines, plusieurs milliers, voire plusieurs dizaines de milliers d'utilisateurs. Si vous voulez éviter un projet informatique long et couteux, il convient que la solution choisie soit la plus simple à déployer. Notamment rien ne devra avoir à être installé sur le poste de travail de l'utilisateur.

Ainsi, la solution déployée dans des délais raisonnables permettra de s'attaquer rapidement au vif du sujet qui est la préparation et le lancement de votre campagne de sensibilisation.

4.9 FACTEUR CLÉ DE SUCCÈS N° 9 : COMMUNIQUER

Les utilisateurs seront d'autant plus enclins à suivre les campagnes de sensibilisation qu'ils auront l'impression de participer à un élan général. Il est donc nécessaire de communiquer autour des opérations de sensibilisation.

On pourra ainsi :

- pré annoncer les opérations de sensibilisation ;
- avoir un mot de la Direction ;
- bien choisir la formule de lancement ;
- effectuer les relances ;
- communiquer sur les résultats, donner du *feed back* aux utilisateurs.

4.10 FACTEUR CLÉ DE SUCCÈS N° 10 : PERSÉVÉRER

Mettre en place une culture cybersécurité prend du temps. Cela ne se pas en un an. Il faut donc persévérer et inscrire son effort dans la durée. Rappelons-le, la sensibilisation n'est pas un projet, c'est un processus.

SEULS 58 % DES 22-37 ANS SAVENT CE QU'EST UN PHISHING CONTRE 73 % DES PLUS DE 54 ANS. LES « DIGITAL NATIVE » SERAIENT-ILS AUSSI DES « DIGITAL NAÏVE » ?

12 rue Vivienne

75002 Paris - France

https://www.conscio-technologies.com

contact@conscio-technologies.com

+33 (0) 184 80 82 00