Cyrius

Tout savoir sur l'engagement collaborateur en cybersécurité

Le guide pratique pour créer une véritable culture cyber, de la PME au grand groupe.

Sommaire

Préface

Maxime Rameau – Co-fondateur & CPO chez HarfangLab

Chez HarfangLab, notre RSSI est en charge de notre cybersécurité. Sa mission est de nous couvrir le mieux possible et de faire les efforts nécessaires pour engager chaque collaborateur.

Il faut tout de même garder en tête que vos collaborateurs doivent travailler avec un niveau de sécurité respectable, sans perdre en efficacité. C'est au département cybersécurité de s'adapter à votre croissance et non l'inverse !

Autre point à noter : il faut savoir éduquer, sans punir ceux qui jouent le jeu.
Cela veut dire qu'une intrusion ne doit pas forcément être considérée comme un échec. Il est de toute façon très difficile pour le RSSI et ses équipes de gérer toutes les menaces en permanence. Cependant, les collaborateurs qui ne participent pas à la protection de l'entreprise (cliquent sur tous les liens des mails ou ne suivent pas les formations, activent des macros sur des documents non légitimes…) ne peuvent pas être laissées sur le côté. Il est essentiel qu'ils comprennent qu'ils représentent la plus grande menace de l'entreprise.

Vous l'aurez compris à travers ces lignes, l'important pour votre entreprise est de garder la bonne posture. Car la sécurité, ce n'est jamais fini : c'est plus un état d'esprit qu'un statut à atteindre.

Heureusement, vous trouverez dans cet ouvrage toutes les clés pour créer et diffuser cette posture sécurité auprès de vos équipes.
Bonne lecture !

Introduction

À la question "Comment engager ses collaborateurs à la cybersécurité ?", il est important de définir clairement ce que le terme "engagement" signifie.

Selon nous, engager un collaborateur dépasse la sensibilisation ou la formation.

Quand une campagne de sensibilisation a pour objectif de partager des bonnes pratiques pour améliorer la vigilance et les compétences, une campagne d'engagement a pour objectif de créer une culture.

Concernant la cybersécurité, engager ses collaborateurs permet de :

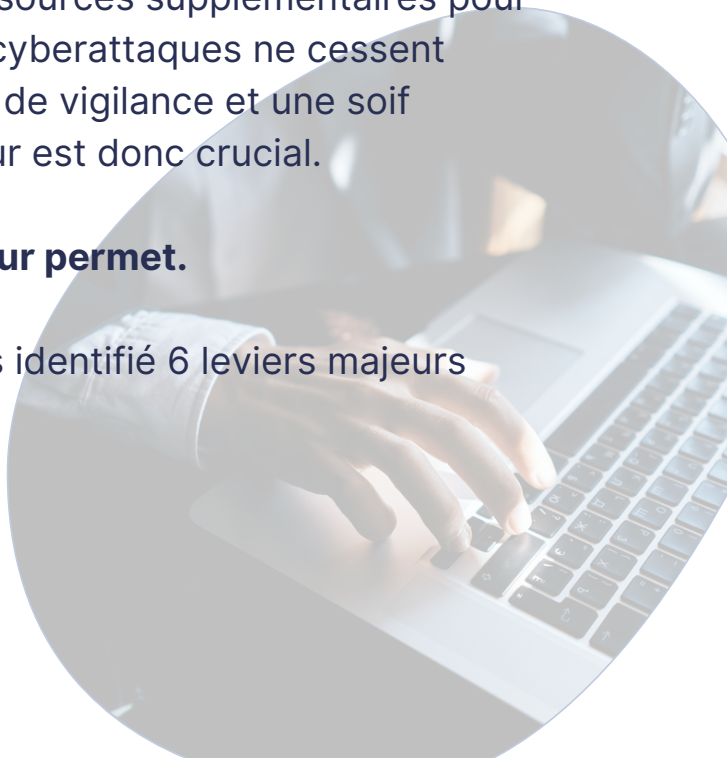
- Faire prendre conscience des dangers encourus
- Faire comprendre le rôle prépondérant de chaque collaborateur (et plus seulement le service IT)
- Créer un effet de groupe, où la cyber devient un sujet dont on parle
- Impliquer des changements de comportement durables

Et ce en plus de simplement faire monter en compétence vos utilisateurs.

La principale raison de dégager des ressources supplémentaires pour engager et non sensibiliser est que les cyberattaques ne cessent d'évoluer. Maintenir un niveau constant de vigilance et une soif d'apprentissage de chaque collaborateur est donc crucial.

C'est ce que l'engagement collaborateur permet.

Pour créer cet engagement, nous avons identifié 6 leviers majeurs développé dans cet ouvrage.



Les Experts

Thierry Allart

RSSI & DPO - Prolival

LinkedIn

Olivier Boidin

RSSI – Clésence

LinkedIn

Maxime Cailleretz

RSSI – Département du Nord

LinkedIn

Yann Gautronneau

RSSI Adjoint – Visiativ

LinkedIn

Grégoire Locqueneux

RSSI – Rhenus Logistics

LinkedIn

Maxime Rameau

CPO – HarfangLab

LinkedIn

Fabian Richard

RSSI – ARS Normandie

LinkedIn

Cédric Simbille

RSSI – Société Générale

LinkedIn

Philippe Steuer

RSSI – Bordeaux Métropole

LinkedIn

Teddy Thalien

Responsable Informatique – Fondation Royaumont

LinkedIn

Steven Vandewalle

RSSI – Splio

LinkedIn

Cédric Voisin

RSSI – Doctolib

LinkedIn

01

Levier #1 Implication au quotidien

Quand on parle d’implication du quotidien, on parle évidemment de la vôtre, mais surtout de la sollicitation des vos équipes sur les sujets cyber.
Et ce de façon régulière, très régulière…

Levier #1 - Implication au quotidien

1.1 La répétition : clé de l'apprentissage

Pour maximiser l'engagement de vos collaborateurs, une bonne pratique consiste à répéter souvent les bonnes pratiques, avec des modules de courte durée. C'est d'ailleurs notre **premier conseil** : éviter les campagnes de sensibilisation annuelles, même semestrielles. Et ce pour deux raisons principales :

1 **Le contenu partagé est en grande partie oublié avant la prochaine campagne**

On oublie en moyenne 60% de ce qu'on apprend 24h plus tard

2 **Le contenu partagé est trop long**

Les capacités de concentration et d'attention profonde ne dépassent pas 30 minutes

Sources : Norman Mackworth, National Training Laboratories

1.2 Utiliser des formats variés

Pour garder un taux de déperdition le plus faible possible, il est nécessaire de maintenir l'intérêt des collaborateurs. Pour cela, une des manières les plus efficaces est de **varier les formats utilisés.**

> **Il faut multiplier les formats et les occasions pour que la sensibilisation soit efficace. La cyber, ce n'est pas qu'en octobre ! On peut organiser des ateliers, des jeux, des communications de toutes formes, des interventions...**
>
> **Maxime Cailleretz, RSSI - Département du Nord**

Quelques exemples de supports à essayer avec vos équipes

- Quiz
- Témoignages de collaborateurs
- Articles
- Vidéos
- Actualités
- Interviews d'experts
- Serious games
- Statistiques du secteur
- Mises en situation

Vous pouvez aussi utiliser des supports physiques, pour maintenir cette vigilance lorsque vos collaborateurs ferment leurs ordinateurs :

- Affiches
- Stickers
- Cache-caméras

1.3 Profiter du temps de travail

> **Il faut absolument que les séances de sensibilisation soient réalisées sur le temps de travail … Mettre le travail en pause pour parler cybersécurité envoie un signal fort : le sujet est suffisamment important pour qu'on bloque un créneau**

Maxime Cailleretz, RSSI - Département du Nord

Il faudra qu'ils comprennent l'importance de ces enjeux et qu'ils aient toutes les ressources nécessaires pour aider leurs équipes. Pour cela, nous recommandons de prendre le temps de leur faire une présentation en amont de votre campagne. Demander l’arrêt du travail pour une réunion avec l’équipe demande inévitablement l’implication des managers et c’est un bon moyen de les avoir de votre côté.

02

Levier #2 Conseils concrets

Comme vos collaborateurs n’ont globalement pas fait d’études en cybersécurité, ils attendent de vous de les prendre par la main. En leur partageant des pratiques simples d’une part, en vulgarisant tout le jargon technique et en leur permettant d’y avoir accès facilement.

2.1 Apporter du contexte : la condition pour impliquer un changement

Vu dans un email de sensibilisation : « Merci d'utiliser un gestionnaire de mot de passe protégé par un mot de passe fort. » Mettons-nous à leur place, qui comprend vraiment ce que ça veut dire ? Pour engager les employés à vos enjeux cyber, ils doivent comprendre l'intérêt de la procédure et n'avoir aucune question à se poser sur ce qu'il faut faire :

Pourquoi ?	**Comment ?**	**Avec quels outils ?**
A partir de quand ?	**Avec quel objectif ?**	**Y a-t'il des failles ?**
Comment est-ce que ça marche ?	**Comment est-ce que ça me protège ?**	**Et si je n'y arrive pas ?**

Autant de questions, et au moins autant de raisons pour eux de laisser tomber. **Rappelez-vous, ce n'est pas leur métier !** Pourtant, il est possible de les impliquer en clarifiant et détaillant les messages que vous souhaitez passer.

> **La cyber est vue comme un sujet de technicien. Il y a un vrai travail de vulgarisation à réaliser**
>
> **Philippe Steuer,**
> **RSSI - Bordeaux Métropole**

Levier #2 - Conseils concrets

2.1 Apporter du contexte : la condition pour impliquer un changement

Exemple

Ce qu'il faut éviter

« Les collaborateurs doivent utiliser un gestionnaire de mot de passe protégé par un mot de passe fort. »

Ce qu'il est possible de faire

« Les collaborateurs doivent utiliser le gestionnaire de mot de passe X à partir du JOUR/MOIS/ANNEE. La décision a été prise suite à la faille de données que l'entreprise a subi il y a 2 semaines. Aussi, l'usage d'un tel outil permettra de sécuriser le partage de mots de passe d'un collaborateur à un autre, les partages par mails et les SMS pouvant être dangereux. Concernant le choix du gestionnaire X, il a été fait au regard de nos procédures de sécurité des données. Un mot de passe fort comporte à minima 10 caractères, ayant des chiffres, majuscules et minuscules, symboles. Il ne doit pas être utilisé pour un autre compte. Pour toute question, le responsable de cette opération est M. PRENOM NOM, joignable par mail à PRENOM@nomdedomaine.com. »

Bien évidemment, il n'est pas nécessaire d'aller systématiquement aussi loin dans l'explication.
*L'idée est simplement d'aider les collaborateurs dans leurs changements de pratique en apportant plus de contexte

> **C'est dans l'incompréhension que les erreurs sont commises.**
>
> **Fabian Richard,**
> **RSSI - ARS Normandie**

2.2 Des ressources facilement accessibles

Avoir une PSSI c'est normal, la partager c'est bien, la rendre aussi disponible dans un Cloud ou sur l'intranet, c'est encore mieux.
Mais vous pouvez aller encore plus loin !

> **J'essaye d'entourer l'utilisateur avec des règles et outils pour qu'il ne soit jamais seul face à l'outil informatique. Il s'agit de placer des bouées de secours quelle que soit la direction où il/elle pourrait aller, afin de rassurer l'utilisateur et de lui faire savoir qu'on est là pour lui.**
>
> **Fabian Richard, RSSI - ARS Normandie**

4 idées pour faciliter l'accès des ressources cyber à vos collaborateurs

1 Adresse email dédiée

Créer une adresse mail dédiée aux problématiques cyber, à utiliser pour partager vos contenus et pour répondre aux questions des collaborateurs (cyber@nomdedomaine.com)

2 PSSI simplifiée

Editer une version simplifiée et compréhensible de la PSSI, et la télécharger sur tous les ordinateurs de l'entreprise. Si possible, héberger la PSSI sur une page web sécurisé, à mettre en favori sur le navigateur des collaborateurs.

3 Multiplier les formats

Varier les formats en imprimant des affiches partageant les bonnes pratiques. Vous trouverez ici les différentes ressources proposées par Cybermalveillance.gouv.fr

4 Interragir directement avec eux

Organiser des foires aux questions/boites à idées (anonymes si nécessaire) et les documenter pour garder une trace

03

Levier #3 Vie pro & vie perso

Il s’agit ici d’un des leviers les plus pertinents pour engager ses collaborateurs. Car là où l’envie de protéger son entreprise peut prendre du temps, il est évident que chacun est plus enclin à se protéger soi-même. Voyons comment tourner l’individualisme à votre avantage.

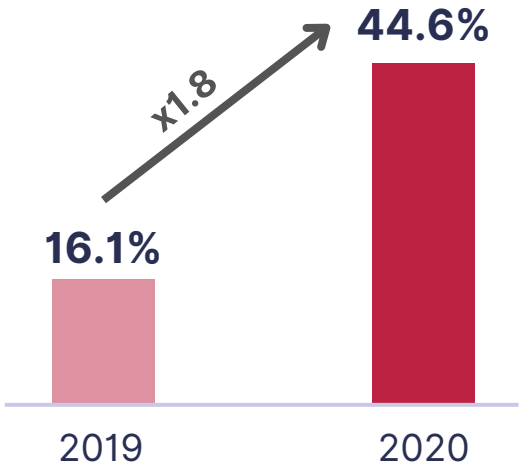
Levier #3 - Vie pro & vie perso

3.1 Le télétravail : l'élément déclencheur

Avant mars 2020, le télétravail et toutes ses contraintes de sécurité existaient déjà. Certains commerciaux devaient se rendre à l'étranger pour un contrat, certains cadres travaillaient chez eux le week-end, etc.

La différence avec le monde d'aujourd'hui, c'est que ces collaborateurs étaient une minorité : 16 % des travailleurs européens de 2019 étaient concernés. Les criminels n'avaient pas pleinement conscience des opportunités liées à cette tendance. En 2020, cette proportion est passée à 45%. Une augmentation de près de x2 en 1 an !

Evolution du travail en Europe



x4 Depuis l'obligation de travailler depuis chez soi, le nombre d'attaques par rançongiciel traitées par l'ANSSI a quadruplé entre 2019 et 2020. Il est devenu comme évident qu'il était plus facile (au moins sur le papier) d'atteindre une entreprise en ciblant les collaborateurs chez eux. Les plus chanceux ont bénéficié d'une formation sur le sujet, et utilisent des outils pour décourager les cybercriminels (utilisation d'un ordinateur pro en plus du perso, VPN, 2FA, Wifi personnel sécurisé...). D'autres malheureusement ont dû apprendre sur le tas, et n'ont bénéficié d'aucune délimitation entre leur vie pro et perso : mêmes appareils, même réseaux, même horaires.

3.2 Le lien vie pro / vie perso

Si on arrive à communiquer les bonnes pratiques pour que les collaborateurs puissent se protéger eux et leur famille, il y a fort à parier que ces bonnes pratiques se retrouveront aussi au travail.

> **Ce n'est pas leur argent, leur travail, leur maison. Il faut leur montrer le lien entre leur vie privée et celle du bureau, car ils ne vont pas le faire d'eux-mêmes !**
>
> **Fabian Richard, RSSI - ARS Normandie**

N'oublions pas, l'objectif est de créer cette culture cybersécurité, d'augmenter cette vigilance dès qu'un collaborateur est en ligne. Quelques exemples choisis :

1. **S'ils utilisent la MFA sur leurs comptes LinkedIn, ils comprendront l'intérêt d'utiliser un tel outil pour leurs comptes pro**
2. **S'ils utilisent un gestionnaire de mots de passe sur leur ordi perso, ils en utiliseront un volontiers sur leur ordi pro**
3. **S'ils utilisent un VPN quand ils prennent le train pour regarder un film, ils utiliseront aussi le VPN de l'entreprise en déplacement professionnel**
4. **S'ils mettent à jour leur téléphone et leur montre connectée, ils mettront aussi à jour leur ordi pro et le logiciel de leur souris**

3.2 Le lien vie pro / vie perso

Bref, si on souhaite déclencher un changement de comportement profond, trouver un exemple similaire dans la vie personnelle peut montrer que ce changement sera bénéfique à la fois à l'entreprise et à eux-mêmes et leurs proches.

Séparer les usages pro/perso, oui, séparer les bons comportements, non !

> **Il faut enseigner la SSI sans que les utilisateurs ne s'en rendent compte. Et pour ça, rien n'est plus efficace que les exemples de la vie personnelle.**

Teddy Thallien, Responsable Informatique - Fondation Royaumont

04

Levier #4 Psychologie et gamification

Les cybercriminels ne se privent pas d'utiliser des éléments irrationnels pour perpétrer leurs attaques. À nous d'utiliser des armes similaires pour s'en protéger !

Levier #4 - Psychologie et gamification

4.1 23% des attaques débutent par de l'ingénierie sociale

Les éléments irrationnels sont une priorité. Toute l'ingénierie sociale est basée sur des éléments de **pression psychologique**. Une autre bonne pratique pourrait être d'axer sa communication sur ces éléments, afin d'empêcher les collaborateurs d'y succomber.

Entraîner ses utilisateurs à reconnaître les éléments de pression psychologique qui sont la caractéristique de l'ingénierie sociale doit faire partie de vos enjeux de sensibilisation !

Quels sont les différents leviers à identifier ?

- Sentiment d'urgence
- Mention d'un gain ou d'une perte
- Position d'autorité
- Abus de confiance

4.2 Utiliser les méthodes des attaquants

Il faut marquer les collaborateurs pour leur faire prendre conscience du risque. Et ça passe par des éléments émotionnels : simplement informer les équipes qu'ils peuvent faire perdre X centaines de milliers d'euros à l'entreprise est une chose, leur envoyer une campagne de faux phishing en leur mettant les conséquences sous les yeux en est une autre.

Même avec une simple campagne de phishing, on peut faire prendre conscience aux utilisateurs de la réalité de la chose. Le dialogue est ouvert et vous pouvez en profiter pour faire passer vos messages.

> **Même avec un budget restreint, on peut lancer des campagnes GoPhish gratuitement**
>
> **Olivier Boidin, RSSI - Clésence**

Attention : Les campagnes de phishing sont UN des nombreux moyens à votre disposition pour engager les collaborateurs. S'ils sont efficaces pour « brûler » vos utilisateurs, ils ne sont pas suffisants à eux seuls pour créer une véritable culture cybersécurité.

> **Les clés USB qui traînent sont aussi un très bon moyen de tester le niveau de maturité des collaborateurs. Et même si c'est une technique un peu old school, c'est encore très efficace et marquant pour les utilisateurs.**
>
> **Yann Gautronneau, RSSI Adjoint Visiativ**

4.3 Utiliser les mécaniques du jeu pour qu'ils s'approprient le message

Les responsables de formation sont parfois découragés en voyant que leurs utilisateurs ne prennent pas les formations de cybersécurité au sérieux, alors que n'importe qui peut passer des heures sur Candy Crush. On se demande pourquoi, quand la majorité des modules proposés sont ennuyeux et/ou trop techniques, ou à l'inverse infantilisants. Pour réellement intéresser les collaborateurs à un sujet, on peut se mettre à leur place et concevoir des contenus qu'ils prennent plaisir à consommer. Et non, ce n'est pas juste parce que c'est une vidéo ou un jeu de plateau que le format plaît.

Les éléments d'une bonne gamification

1 **Fixer des objectifs de formation clairs et des moyens de les atteindre**

Exemple : « La SSI est un enjeu important pour SpaceX car une cyberattaque peut nous coûter 15 millions. Pour éviter cela, vous devez réaliser 6 modules par mois pendant 3 mois. »

2 **Définir des règles précises**

Exemple : « Au-delà du 15 avril, vous ne pourrez plus accéder à votre messagerie si vous n'avez pas complété la formation »

4.3 Utiliser les mécaniques du jeu pour qu'ils s'approprient le message

3 **Montrer à l'utilisateur que sa participation est prise en compte** (voir Levier # 5)

Exemple : « Bravo pour votre participation du jour, vous avez progressé de 5% vers votre objectif. Souhaitez-vous poser une question ? »

4 **Donner une raison de rester motivé**

Exemple : « La prochaine fois, vous verrez comment éviter une fraude à la carte bleue. Pratique pour votre vie personnelle ! »

5 **Distribuer des récompenses (intrinsèques ou non)**

Exemple : « Vous avez gagné 10 points sur cette session. À 100 points, vous bénéficiez d'un ticket restaurant supplémentaire sur votre compte mensuel »

4.3 Utiliser les mécaniques du jeu pour qu'ils s'approprient le message

> **Un diplôme est aussi une bonne récompense à donner à la fin d'une formation. Cela a le double avantage de servir pour une certification et de donner à l'utilisateur une raison d'être fier.**

Teddy Thallien, Responsable Informatique - Fondation Royaumont

6 **Donner une liberté de choix à l'utilisateu**

Exemple : « Souhaitez-vous aborder l'exemple 1 ou 2 ? »

7 **Trouver l'équilibre entre valider les acquis et permettre à l'utilisateur d'échouer**

Exemple : « Dommage, c'est perdu pour cette fois. Mais le principal est de s'améliorer, revenez dans quelques jours ! »

05

Levier #5
À l'écoute des collaborateurs

La communication, c’est dans les deux sens. Vouloir pousser des informations ou des actualités sans se pencher sur le ressenti de vos collègues, c’est potentiellement les laisser plonger dans des erreurs facilement évitables.
Sortez vos carnets, pour une fois, on laisse la parole aux équipes.

Levier #5 - À l'écoute des collaborateurs

5.1 Communication interne

On demande souvent aux collaborateurs d'écouter des conseils ou des consignes, mais l'inverse est rarement vrai. Quand avez-vous demandé leur avis à vos utilisateurs pour la dernière fois ?

Être ludique et amusant en réunion de sécurité est une première étape, mais on peut aller plus loin !

> **Il faut être à l'écoute de ses collaborateurs si on veut que les informations transmises soient entendues.**

Thierry Allard, RSSI & DPO - Prolival

> **Etre au contact permanent des équipes métier, ça revient aussi à dire que le RSSI est un psy.**

Fabian Richard,
RSSI - ARS Normandie

Quand on laisse les utilisateurs s'exprimer au sujet de leur expérience personnelle en sécurité informatique, on se rend compte qu'ils ont beaucoup d'anecdotes à partager. Pour certains professionnels, le rôle du responsable cyber est même de faire comprendre le lien entre les mésaventures personnelles et les risques au bureau.

5.1 Communication interne

> **Avoir plus d'informations sur les collaborateurs permet de mieux adapter le discours. L'idéal, c'est de pouvoir adapter le discours en fonction du poste, du niveau hiérarchique...**

Yann Gautronneau, RSSI Adjoint - Visiativ

Le responsable SSI peut passer du rôle de donneur de leçon à celui de conseiller, ce qui présuppose une écoute préalable des besoins des utilisateurs !

Exemple : Pourquoi les utilisateurs utilisent les mêmes mots de passe partout ? En écoutant les doléances des collaborateurs, on se rend compte qu'il est IMPOSSIBLE de retenir tous les mots de passe de notre quotidien. Pourquoi dès lors ne pas mettre en place un gestionnaire de mots de passe ?

5.2 Ne pas passer pour celui qui dit non à tout

La communication et l'empathie sont cruciales pour un sujet aussi anxiogène et omniprésent que la sécurité informatique. Créer du lien avec les utilisateurs permet de développer une relation de confiance

> **Il est très important de rester au contact du terrain pour ne pas passer pour un enquiquineur.**
>
> **Steven Vandewalle, RSSI - Splio**

Mettez-vous à leur place : pourquoi s'intéresser à ce sujet obscur et effrayant de surcroît ? Comment créer de l'intérêt quand on ne connaît pas les motivations et les freins des principaux intéressés ?
-> **Il faut parvenir à créer du dialogue.**

> **Ce qui est certain, c'est qu'il faut que le format plaise pour que la sensibilisation soit efficace. Mais on ne sait pas d'office ce qui plaît... Le mieux est d'aller demander directement.**
>
> **Cédric Simbille, RSSI – Société Générale**

06

Levier #6 Création d'une équipe

Comme tout responsable sécurité qui se respecte le dira, la SSI est un sport d’équipe avant tout. Les surfaces d’attaque explosent, personne n’est en mesure de tout contrôler.
Comment parvenir à déléguer la responsabilité et surtout à transmettre cet état d’esprit de sécurité autour de nous ?
C’est ce que nous voyons dans ce chapitre.

6.1 Jouer collectif

> Moi je représente le RSSI, le gardien des règles "d'en-haut". Ce que je dis sera forcement moins bien pris que si ça vient d'un collègue ou d'un proche.

Philippe Steuer, RSSI – Bordeaux Métropole

> Il y a deux messages essentiels à faire passer aux collaborateurs : 'Chacun est important' et 'Vous n'êtes pas seul'.

Grégoire Locqueneux, RSSI – Rhenus Logistics

Chaque utilisateur est essentiel dans le dispositif de défense, car tous ces soldats au bouclier levé forment un mur difficile à percer.
L'objectif est de développer une **bienveillance collective**, qui se transforme en co-vigilance. Chacun se transforme ainsi en mini-responsable de sécurité qui veille à ce que ses collègues soient protégés également. Exit donc les politiques de pointage du doigt, le but est de parvenir à développer la défense collective. La proximité et les échanges en sont les mécanismes les plus efficaces.

Communiquez un peu plus sur la bienveillance entre collègues. Un collaborateur laisse son ordinateur ouvert en partant en pause ? Et si vous le verrouilliez à sa place, en laissant un mot aimable ?

L'effet de groupe est un levier très puissant de l'engagement : le sentiment d'appartenance à l'entreprise est extrêmement important dans le processus. En se sentant pleinement intégré au groupe, l'utilisateur se donne également pour mission de le protéger.

6.2 Utiliser la hiérarchie

D'autant que si tout le monde le fait, il est bien plus facile de se convaincre que c'est important. Mais pour cela, il faut parvenir à créer l'exemple.

Pourtant ce sont eux qui devraient être les premiers convaincus par le risque !

> **Pour convaincre les directions, il faut souvent sortir une analyse du BCG…**

Cédric Simbille,
RSSI – Société Générale

> **C'est une question d'état d'esprit, qui doit partir d'en haut.**

Cédric Voisin, RSSI – Doctolib

Il faut que la hiérarchie donne le diapason pour que cela déteigne sur le reste de l'entreprise. Les « techniciens » ne sont pas les seuls concernés !

Et c'est là une **condition sine qua non** de l'engagement des collaborateurs : que chaque département, et manager, prenne la responsabilité des sujets sécurité.

Prenons l'exemple de Doctolib : le département SSI commence par créer les process et les transmet aux équipes opérationnelles. Ce sont sont ensuite elles qui sont garantes de la bonne application des consignes. En clair, chaque unité gère sa propre sécurité.
Et ça marche, puisque les collaborateurs sont poussés par leur manager de terrain à appliquer les principes de sécurité

> **Chez nous, les agents sont des "super-héros de la SSI". On entretient cette idée que chacun peut et doit faire sa part du travail**

Maxime Cailleretz, RSSI – Département du Nord

Conclusion

Prendre enfin le risque humain au sérieux

Les directions SI et SSI sont depuis quelques années pleinement conscientes de leur rôle face aux cyberattaques. Si des solutions techniques suffisaient auparavant pour contrer la grande majorité des attaques, ce n'est plus le cas aujourd'hui. La technique se doit maintenant d'être agrémentée d'un volet humain. Où chaque collaborateur prend conscience du danger, de son rôle à jouer et applique les bonnes pratiques partagées par son responsable. Où la cybersécurité fait partie de la culture de l'entreprise.

Pour créer cet engagement, il existe une infinité de solutions. Nous avons tenté d'en présenter les plus efficaces dans cet ouvrage, mais elles seront mises en place en vain si ces trois conditions ne sont pas respectées :

- Les collaborateurs sont accompagnés humainement et en terme de ressources,
- Les managers servent de levier de communication auprès des collaborateurs,
- La direction soutient la démarche et donne aux décideurs SSI la liberté nécessaire.

Ces deux derniers points permettront notamment aux décideurs SSI de (re)gagner la confiance et le pouvoir d'action nécessaires pour accomplir leur mission.
Nous n'avons pas de doute qu'avec ces idées, ils pourront passer du statut de ceux qui imposent les procédures à celui des garants de la sécurité des entreprises. Car finalement, c'est bien ce rôle-là qu'ils méritent.

À propos

Utiliser la technologie pour donner aux collaborateurs les moyens de se défendre.

Chez Cyrius, nous pensons que la sensibilisation à la sécurité est dépassée et inefficace, et nous voulons changer ça. Les organisations et leurs équipes méritent la meilleure protection.

C'est pour cela que nous développons un nouveau type d'interaction avec vos collaborateurs pour faire de la sécurité une responsabilité partagée.

Grâce à 3 piliers complémentaires, la plateforme permet aux responsables sécurité de maintenir un niveau de vigilance élevé tout au long de l'année. Le tout dans une plateforme basée en France, à la technologie propriétaire et souveraine.

Si vous pensez que notre méthodologie pourrait vous aider, n'hésitez pas à nous contacter à achille@cyrius.co.

À très vite !