Le facteur humain en cybersécurité : transformer les faiblesses en forces

Livre électronique

WeActis
par Mondata

Habiliter les employés à renforcer la sécurité de l'entreprise

Le monde de la cybersécurité a évolué, mais une faiblesse fondamentale persiste : le comportement humain.

Les formations traditionnelles de sensibilisation à la cybersécurité mettent souvent l'accent sur la conformité plutôt que sur l'amélioration des comportements durables des employés.

Le présent livre électronique examine les causes pour lesquelles les méthodes traditionnelles sont inadéquates, et présente une approche stratégique pour transformer la sensibilisation à la cybersécurité en une pratique axée sur les comportements et la réduction des risques.

Ce que vous apprendrez

Les lacunes des formations traditionnelles

Les limites des programmes axés sur la conformité et leur incapacité à favoriser le changement de comportement à long terme.

Les raisons de l'erreur humaine en cybersécurité

Surcharge cognitive, facteurs d'oublis et nécessité de mesurer les changements de comportements.

La clé d'une culture de sécurité efficace

Stratégies pour encourager les employés à adopter les bonnes actions sécuritaires grâce à des notifications contextualisées.

Des approches concrètes pour les chefs de la sécurité et des TI

Bien choisir ses indicateurs pour mesurer les progrès et comment engager les employés pour bâtir une culture de sécurité.

En adoptant ces recommandations, les chefs de la sécurité peuvent passer d'une approche centrée sur la conformité à une véritable culture de sécurité durable, où les employés sont pleinement engagés dans la réduction des risques.

Le virage en cybersécurité : de la conformité au changement de comportement

Le monde de la cybersécurité a connu une transformation importante au cours des dernières années. La nécessité d'adopter des mesures robustes et proactives en matière de cybersécurité devient de plus en plus évidente. En effet, des organisations de toutes tailles sont aux prises avec un volume important de cybermenaces, qui évoluent rapidement. Parallèlement, la pénurie de professionnels qualifiés en cybersécurité a incité les entreprises à réévaluer leur approche de la gestion des risques et à **se concentrer davantage sur l'habilitation de leurs employés afin de créer une ligne de défense contre les menaces.**

Une lacune importante persiste malgré les menaces croissantes : le comportement des employés.

69 %

Un sondage réalisé par Gartner en 2024 a révélé que **69 % des employés ont ignoré ou contourné les protocoles de cybersécurité de leur organisation au cours de l'année précédente**, et que 74 % les contourneraient sciemment à des fins professionnelles.

Les statistiques qui précèdent révèlent une grave lacune dans les méthodes de formation traditionnelles qui mettent l'accent sur l'acquisition de connaissances, mais qui ne permettent pas de changer suffisamment le comportement.

Le problème n'est pas simplement un manque de connaissance.

Il s'agit d'un problème systémique plus profond, à savoir l'incapacité de créer des changements comportementaux à long terme relativement aux technologies de l'information et à la cybersécurité chez les employés. Les organisations doivent délaisser les programmes traditionnels fondés sur la conformité pour adopter des stratégies qui favorisent des comportements durables en matière de cybersécurité. Le présent livre électronique réalise une évaluation critique des méthodes classiques, et propose **des stratégies concrètes pour accélérer les efforts de réduction des risques au sein de l'organisation.**

Chapitre 1

L’état actuel des programmes de sensibilisation à la cybersécurité

L’essor de la formation axée sur la conformité

Pendant des années, les programmes de sensibilisation à la cybersécurité ont été principalement conçus pour répondre aux exigences de conformité imposées par des cadres comme la loi 25 sur la protection des données et les normes ISO 27001 et SOC 2. Bien que ces cadres normatifs et législatifs aient été essentiels à la standardisation et à l’accélération des pratiques de cybersécurité, ils ont involontairement amené les organisations à se concentrer sur la préparation aux audits plutôt que sur la création de changements significatifs.

Une culture de conformité n’est pas synonyme d’une culture de sécurité.

La formation axée sur la conformité adhère habituellement à un modèle rigide et universel qui exige que les employés suivent des modules désignés ou passent une série de tests pour respecter les normes de conformité. Malheureusement, ces initiatives sont souvent dissociées des problèmes réels que vivent les employés au quotidien. Il est rare que ces programmes proposent des contextes pertinents et invitent les participants à appliquer leurs connaissances aux menaces réelles, de sorte que ceux-ci sont pris au dépourvu lorsque de véritables risques en matière de cybersécurité se présentent.

Bien que ces programmes puissent aider les organisations à respecter les exigences réglementaires, ils ne font pas toujours la promotion d’une culture de cybersécurité résiliente. Bien souvent, ils sont peu personnalisés, **ce qui entraîne le désengagement des employés.**

Les méthodes de formation traditionnelles

Quelles sont les lacunes?

Bien que les méthodes traditionnelles de formation à la sensibilisation soient répandues, elles se sont révélées insuffisantes pour s'attaquer aux causes profondes des incidents de sécurité.

Voici certaines pratiques courantes :

Modules d'apprentissage numérique

Il s'agit de modules de formation flexibles et asynchrones qui peuvent être suivis à distance, ce qui les rend plus accessibles. Cependant, ils s'appuient souvent trop sur des concepts abstraits et ont tendance à négliger les liens entre les connaissances théoriques et les scénarios pratiques réels.

Simulations d'hameçonnage

Bien que les simulations d'hameçonnage soient une approche courante pour évaluer la susceptibilité aux attaques par courriel, elles se concentrent bien souvent sur la capacité des employés à reconnaître les escroqueries sans tenir compte des tendances comportementales sous-jacentes qui entraînent les gestes risqués.

Campagnes de sensibilisation

Il s'agit de campagnes qui mettent en lumière des thèmes de sécurité précis, comme les politiques relatives aux mots de passe ou les menaces d'hameçonnage, mais qui ont tendance à être sporadiques et ne prévoient pas un renforcement continu, ce qui réduit leur efficacité à long terme.

Signaux environnementaux

Les rappels visuels comme les affiches visent à renforcer les pratiques de sécurité. Cependant, ils sont généralement passifs et les employés tendent à ne plus leur prêter attention une fois qu'ils s'habituent à l'environnement.

Malgré leur utilisation répandue, ces méthodes ne produisent souvent pas de changements comportementaux durables. Les employés peuvent réussir un cours ou même prendre part à une simulation d'hameçonnage, mais sans contexte ou renforcement continu, il est peu probable qu'ils mettent en œuvre leurs apprentissages dans des situations réelles.

Les limites des approches traditionnelles

Les erreurs humaines persistantes

L'erreur humaine continue d'être l'une des principales causes des **atteintes à la cybersécurité.** Même en présence de programmes de formation exhaustifs, les employés commettent toujours des erreurs qui mettent en péril la posture de sécurité de leur organisation. Ces erreurs sont attribuables en partie aux lacunes des méthodes de formation traditionnelles, qui ne tiennent pas compte de la complexité du comportement humain.

Une étude du *National Institute of Standards and Technology* (NIST) a révélé que 84 % des organisations mesurent la réussite en fonction du taux d'achèvement des cours et des résultats aux tests d'hameçonnage.

Bien que ces mesures soient utiles pour suivre la participation des employés à la formation, elles **ne sont pas des indicateurs représentatifs de changements comportementaux réels.** La réussite doit être évaluée en fonction de la réaction des employés devant une menace éventuelle, et non simplement en fonction du choix de cliquer ou pas sur un lien d'hameçonnage durant un test.

84 %

des organisations mesurent la réussite en fonction du taux d'achèvement des cours et des résultats aux tests d'hameçonnage.[1]

1. *National Institute of Standards and Technology* (NIST), étude intitulée "Measuring the Effectiveness of U.S. Government Security Awareness Programs."

La surcharge cognitive et les oublis

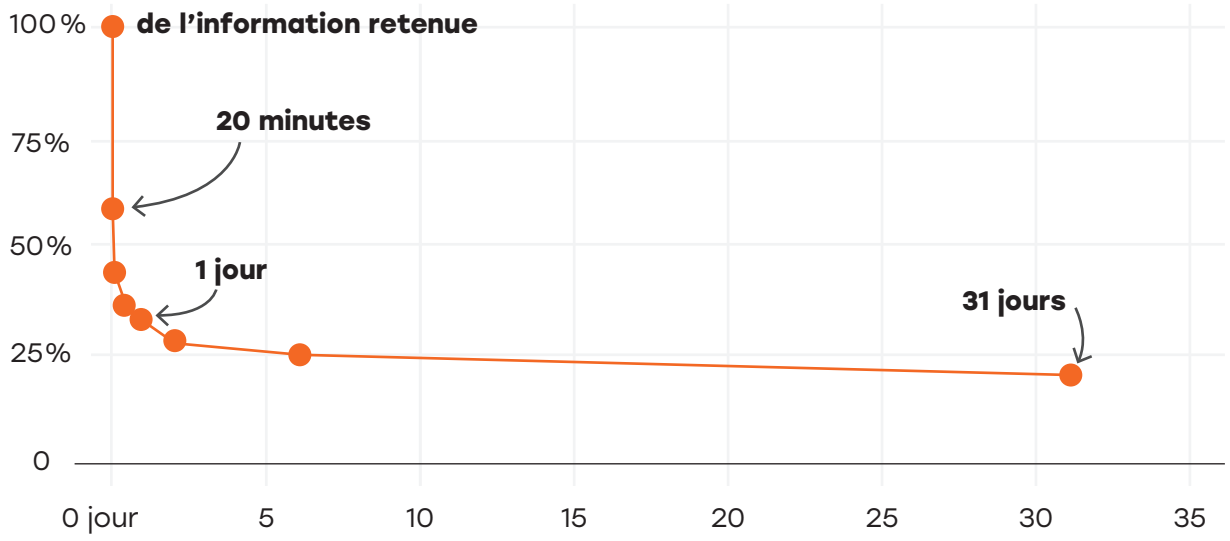
La courbe de l'oubli d'Ebbinghaus[2] est un concept établi en sciences cognitives qui **illustre la vitesse à laquelle l'information peut être oubliée au fil du temps, surtout en l'absence de renforcement.**

Les méthodes de formation traditionnelles prévoient habituellement des séances ponctuelles où les employés doivent mémoriser et appliquer beaucoup d'information sans aucun autre renforcement. Il peut arriver que le résultat soit une surcharge informationnelle, où les employés sont submergés d'information et n'ont pas suffisamment de temps ou d'espace pour assimiler et retenir les concepts essentiels.

De plus, sans mises à jour ou rappels réguliers, les employés oublient rapidement les protocoles de sécurité qu'ils ont appris, ce qui rend la séance de formation initiale presque inutile après peu de temps.

80 % de l'information apprise peut être oubliée en moins d'un mois en l'absence de rappels réguliers.

Courbe de l'oubli d'Hermann Ebbinghaus



2. Courbe d'Ebbinghaus : Comment mieux mémoriser ce que l'on apprend? – Everlaab

L’absence de suivi des comportements

Une autre lacune importante des programmes traditionnels de sensibilisation à la sécurité est **l’absence de suivi après la formation.** Après avoir terminé un cours ou un test d’hameçonnage, il arrive souvent que les employés n’aient pas d’évaluation continue de la mise en pratique de leurs connaissances.

En l’absence d’évaluations comportementales après la formation, si par exemple un employé continue d’utiliser des mots de passe faibles ou de faire fi des recommandations relatives à l’authentification multifactorielle, l’organisation ne s’en rendra pas compte.

La surveillance comportementale peut fournir des **renseignements précieux** pour comprendre si les employés respectent réellement les pratiques sécuritaires et contribuer à cerner les aspects qui nécessitent plus de formation.

L’écart par rapport aux situations réelles

Les méthodes de formation traditionnelles sont souvent insuffisantes parce qu’**elles ne se fondent pas sur un contexte réel** dans le quotidien de l’employé. Les leçons théoriques ou les documents statiques, comme les diaporamas et les affiches, demeurent sans écho auprès des employés. La sensibilisation à la sécurité est plus efficace lorsque la formation pratique repose sur des situations réelles personnalisées au contexte de l’employé.

En effet, les employés sont plus susceptibles de se souvenir des protocoles de sécurité lorsque l’apprentissage est fondé sur des exercices où les cas de figure proposés correspondent à des difficultés qu’ils doivent affronter dans l’exercice de leurs fonctions au quotidien. Il s’agit d’une approche qui éveille tout leur intérêt et leur permet de **s’exercer à prendre les bonnes décisions dans un environnement à faible risque** avant de les appliquer dans des situations à risque élevé.

Les recommandations stratégiques pour les chefs de la sécurité

Les chefs de la sécurité doivent aller au-delà des programmes traditionnels de sensibilisation à la cybersécurité et adopter une stratégie fondée sur les comportements et les données afin de réduire les risques. Pour parvenir à un changement durable, il faut améliorer la méthode d'évaluation des comportements cybersécuritaires, adapter la formation en matière de sécurité et offrir des solutions pratiques et stimulantes qui favorisent la participation à long terme des employés.

1

Revoir les indicateurs

Passer de la conformité à des indicateurs comportementaux significatifs

Les programmes traditionnels de sensibilisation à la sécurité évaluent souvent le succès en faisant le suivi des taux d'achèvement des formation, des taux de clics d'hameçonnage ou du nombre d'incidents signalés. Ces mesures donnent un aperçu de l'engagement, certes, mais elles ne permettent pas d'évaluer les changements de comportement ou de surveiller l'amélioration continue des pratiques de sécurité.

Les chefs de la sécurité devraient se concentrer sur les aspects suivants :

Les indicateurs comportementaux de sécurité

Plutôt que de simplement surveiller les taux d'achèvement, évaluer la fréquence à laquelle les employés mettent en œuvre les principes de sécurité dans des situations pratiques, notamment en examinant :

- le taux d'échange sécurisé de fichiers dans les plateformes infonuagiques;
- la croissance du nombre d'employés qui utilisent des mesures d'authentification rigoureuses (authentification multifactorielle, gestionnaires de mots de passe ou autres outils offerts);
- la diminution des infractions aux politiques au fil du temps (ex. moins de données mal configurées dans Microsoft 365).

L'évaluation adaptative du risque

Prévoir un modèle d'évaluation du risque qui s'adapte en fonction du comportement des employés au fil du temps. Par exemple, les employés qui signalent constamment les courriels d'hameçonnage et qui suivent les protocoles de sécurité devraient être classés dans la catégorie à faible risque. En revanche, une personne qui contourne souvent les politiques peut nécessiter une formation ciblée et représenter un risque plus important.

La gestion contextualisée des risques

Utiliser les indicateurs comportementaux pour permettre aux équipes de sécurité de repérer les départements à risque élevé et personnaliser les interventions en matière de sécurité.

2

La formation contextualisée de sécurité

Rendre la cybersécurité pertinente et réalisable

Les employés sont plus susceptibles d'adopter des mesures de sécurité lorsqu'ils voient directement leur **pertinence dans leur travail de tous les jours.** Les chefs de la sécurité devraient délaisser la formation générique, et prendre les mesures suivantes :

Les conseils en matière de sécurité en fonction des rôles

La formation sur la sécurité doit être adaptée aux rôles et aux situations pratiques propres à chaque poste.

- **Équipes des finances :** Reconnaître l'ingénierie sociale dans la fraude liée aux factures.
- **Équipes des ressources humaines :** Repérer les menaces internes et protéger les renseignements permettant d'identifier une personne.
- **Équipe des technologies de l'information :** Réduire les erreurs de configuration dans les environnements infonuagiques.

Les notifications de sécurité fondées sur le principe du « coup de pouce »

Au lieu de miser sur une formation annuelle, donner des conseils en matière de sécurité en temps réel dans les flux de travail.

- **Exemple 1:** Si un employé est sur le point de transmettre un document de nature délicate à l'externe, déclenchez une alerte de sécurité dans l'application, qui explique les bonnes pratiques.
- **Exemple 2:** Si un employé oublie d'activer l'authentification multifactorielle, affichez un guide pour expliquer rapidement les raisons pour lesquelles il faut corriger la situation et la façon de le faire.

Les exercices de simulation d'intervention en cas d'incident

Aller au-delà des simulations statiques d'hameçonnage et mettre en œuvre des exercices interactifs où les employés peuvent s'exercer à prendre des décisions sous pression dans des mises en situation de cybermenaces réelles.

3

L'encouragement aux prises d'actions

Inciter les employés à devenir des contributeurs de la sécurité

Pour promouvoir une culture axée sur la sécurité, les organisations doivent éduquer les employés sur les bonnes pratiques à adopter selon leur contexte particulier et leurs permettre ensuite de prendre facilement action.

Le programme des champions de la sécurité

Recruter des contributeurs exemplaires de la sécurité à l'interne, au sein des divers services, et les former pour qu'ils promeuvent les meilleures pratiques en matière de sécurité auprès de leurs pairs.

La ludification et les incitatifs

Prévoir des défis stimulants, des tableaux de classement et des récompenses pour les employés qui adoptent des comportements proactifs en matière de sécurité (p. ex., taux de détection d'hameçonnage le plus élevé, mise en œuvre de la plupart des recommandations relatives à la sécurité). Certaines organisations ont commencé à intégrer graduellement ces nouvelles mesures dans les grilles de performance et dans les évaluations des employés.

Les renseignements sur les menaces qui proviennent des employés

Inciter les employés à signaler les incidents de sécurité et partager leurs la façon dont leurs contributions ont permis de réduire les risques.

En redéfinissant les indicateurs pour mieux mesurer les changements de comportements, et en proposant des formations contextuelles ainsi que des actions sécuritaires simples, les responsables de la sécurité peuvent **instaurer une culture durable où les employés deviennent des acteurs engagés dans la réduction des risques,** plutôt que de simples participants passifs aux formations.

Les points à retenir

La formation traditionnelle est insuffisante →	Les programmes axés sur la conformité sensibilisent les gens, mais ne changent pas leurs comportements.
Le changement de comportement est essentiel →	Les employés ont besoin de renforcement et de mise en contexte personnalisée pour rester engagés.
La nécessité de nouvelles mesures pour évaluer l'amélioration des comportements →	Il faut passer des taux d'achèvement à des indicateurs comportementaux qui attestent des améliorations tangibles en matière de sécurité.
La personnalisation accroît l'efficacité →	La formation en fonction des rôles, les notifications en temps réel (« coups de pouce ») et l'apprentissage personnalisé améliorent l'engagement.
L'engagement favorise le changement de culture →	La sécurité doit être intégrée au quotidien grâce à la ludification, aux incitatifs et aux programmes dirigés par les pairs.

Pour débuter

1 **Réévaluer son approche de formation en matière de sécurité**

Évaluer le programme actuel pour repérer les lacunes dans le renforcement des comportements.

2 **Mettre en œuvre des mesures comportementales**

Surveiller les habitudes relatives à la sécurité, et non seulement du taux d'achèvement de la formation.

3 **Envoyer des notifications de sécurité en temps réel**

Notifier les employés lors d'un comportement à risque pour leurs permettre de le corriger rapidement.

4 **Lancer un programme de champions de la sécurité**

Habiliter les employés à promouvoir la sécurité au sein de leur service.

5 **Ludifier l'engagement pour ce qui est de la sécurité**

Se servir de tableaux de classement, de défis et d'incitatifs pour promouvoir un comportement exemplaire en matière de sécurité.
Rendez cela agréable !

À propos de WeActis

WeActis révolutionne la cybersécurité en transformant les employés en contributeurs actifs, et en faisant de la sécurité une responsabilité collective, et non pas un fardeau informatique.

Intégrée à Microsoft Teams, l'application **WeActis** encourage les employés à prendre des actions sécuritaires simples permettant de diminuer les risques de leur organisation en moins de cinq minutes par semaine.

En favorisant une meilleure hygiène des données dans Microsoft 365, en renforçant la gouvernance et en simplifiant la gestion des risques, **WeActis** permet aux organisations de bâtir une culture de cyberrésilience. Cela se traduit par une meilleure conformité, une réduction de l'exposition des données et des améliorations en sécurité, à la fois mesurables et durables.

info@weactis.com
1 833 666-3282
WeActis.com

WeActis
par Mondata