sosafe

5 métriques pour démontrer le ROI de votre stratégie de cybersécurité

Comment prouver au board que votre programme de sensibilisation rapporte plus qu'il ne coûte.

www.sosafe-awareness.com/fr

Contenu

Introduction 3

Les 5 métriques essentielles en un coup d'œil 3

Métrique 1 : Réduction du risque d'erreur humaine 4

Métrique 2 : Coût des incidents évités 5

Métrique 3 : Taux de détection et signalement 6

Métrique 4 : Score de conformité réglementaire (%) 7

Métrique 5 : Ratio d'efficacité du programme 8

Conclusion - Votre prochaine présentation au board : mode d'emploi 9

5 métriques ROI que votre board ne pourra pas ignorer

Voici 5 métriques qui transforment vos résultats de sensibilisation en euros économisés et en risques évités. Des arguments concrets pour votre CFO.

Votre conseil d'administration se fiche de savoir que 87 % des employés ont suivi la formation cybersécurité. Ce qu'ils veulent savoir : combien d'incidents avez-vous évités ? Combien d'euros avez-vous économisés ? Le risque a-t-il vraiment diminué ?

C'est logique : **les boards pensent en termes de risques business et de retour sur investissement** Pas en taux de complétion ou en scores de quiz.

Le problème ? **La plupart des RSSI continuent de présenter des métriques opérationnelles qui ne disent rien sur l'impact financier réel.** Résultat : la sensibilisation reste vue comme un mal nécessaire, pas comme un investissement stratégique.

Ce guide vous donne cinq métriques qui changent tout. Des indicateurs qui parlent directement le langage du board : réduction mesurable des risques, économies chiffrées, ROI démontrable. De quoi transformer votre prochain reporting en argument massue pour votre budget 2025.

Les 5 métriques essentielles en un coup d'œil

1. Réduction du risque d'erreur humaine
2. Coût des incidents évités
3. Taux de détection et signalement
4. Score de conformité réglementaire
5. Ratio d'efficacité du programme

1 Réduction du risque d'erreur humaine

Ce que ça mesure :

La part d'employés qui présentent encore un risque après vos campagnes de sensibilisation. On ne compte pas seulement les clics sur un email : on mesure toute action non sécurisée (clic sur un lien malveillant, partage d'identifiants, téléchargement interdit, etc.) détectée lors des tests et simulations.

Pourquoi c'est important :

Chaque action évitée peut représenter un incident en moins (phishing, ransomware, fuite de données). Cette métrique prouve l'efficacité directe de vos programmes de formation.

Comment la calculer :

1. **Calculez d'abord le taux initial :**

nombre d'actions non sécurisées ÷ nombre total d'expositions aux tests.

Exemple : 84 actions à risque sur 1 200 tests = **7 %.**

2. **Répétez ensuite la mesure à la période suivante.**

3. **Appliquez la formule :**

(taux initial – taux actuel) ÷ taux initial ✕ 100.

Exemple : un passage de 22 % à 7 % correspond à une réduction de **68 %.**

Message pour le board :

« Nos employés sont 3 fois moins susceptibles de déclencher un incident qu'il y a un an. »

2 Coût des incidents évités

Ce que ça mesure :

l'argent que vous n'avez PAS dépensé en gestion de crise grâce à la réduction des incidents. Chaque attaque évitée = des centaines de milliers d'euros économisés en investigation, remédiation, perte d'activité, amendes RGPD.

Pourquoi c'est important :

« Pour chaque euro investi dans la sensibilisation, nous économisons X euros en incidents évités. » Voilà un argument qui fait valider les budgets sans discussion. Cette approche s'inspire de la méthode de la pyramide inversée utilisée notamment par le CISO de Goldman Sachs : au sommet se trouvent toutes les attaques potentielles, et à la base le nombre infiniment plus faible d'incidents réels grâce au déploiement des contrôles, comme la sensibilisation.

Comment la calculer :

1. **Identifiez vos principaux types d'incidents coûteux liés au facteur humain** (ex : BEC, ransomware via phishing).

2. **Pour chacun, calculez la fréquence annualisée de référence avant les améliorations du programme et la fréquence actuelle.**

3. **Multipliez la différence par un coût conservateur par incident (de vos propres données ou de références sectorielles fiables).**

4. **Additionnez tous les types d'incidents pour obtenir le coût total évité.**

Exemple : 2,7 M€ de pertes évitées sur 12 mois grâce à la réduction des incidents (ransomware, fraude au président, fuites de données).

Message pour le board :

« Notre investissement de 350 000 € en sensibilisation a évité 2,7 M€ de pertes. ROI : 770 %. »

3 Taux de détection et signalement

Ce que ça mesure :

le pourcentage d'employés qui détectent ET signalent une menace avant qu'elle ne fasse des dégâts. Plus important : la vitesse de signalement. Car quinze minutes ou trois jours, cela change tout.

Pourquoi c'est important :

chaque minute gagnée = des milliers d'euros économisés en limitation des dégâts. Un employé qui signale rapidement une menace, c'est un SOC qui intervient avant la propagation, c'est une attaque stoppée net.

Comment la calculer :

1. **À partir des simulations et des journaux d'incidents réels, comptez les menaces que les employés ont correctement signalées.**

2. **Divisez par le total des menaces auxquelles ils ont été exposés = taux de détection/signalement.**

3. **Suivez le temps médian de signalement pour un contexte supplémentaire.**

Exemple : 74 % des tentatives de phishing signalées dans les quinze minutes suivant la réception.

Message pour le board :

« Nos employés stoppent trois attaques sur quatre avant qu'elles ne deviennent des incidents. Notre temps de réaction est passé de trois jours à quinze minutes. »

4 Score de conformité réglementaire (%)

Ce que ça mesure :

l'alignement réel entre les comportements de vos employés et les exigences réglementaires. NIS2, ISO 27001, DORA : chaque norme a ses obligations de sensibilisation. On mesure, on prouve, on documente.

Pourquoi c'est important :

pas d'amende = argent économisé. Audit réussi du premier coup = pas de coûts de remédiation en urgence. Mais surtout, une conformité documentée et mesurable, c'est l'assurance de ne pas voir l'entreprise en une des journaux pour les mauvaises raisons.

Comment la calculer :

1. **Listez tous les comportements de sécurité réglementaires requis du personnel** (ex : compléter des modules spécifiques, réussir des tests de politique).

2. **Suivez les taux de complétion/réussite dans toute l'organisation.**

3. **Exprimez en pourcentage, pondéré si certaines exigences sont prioritaires.**

Exemple : 94 % du personnel a complété les modules obligatoires avant l'audit NIS2.

Message pour le board :

« Nous sommes à 94 % de conformité NIS2. L'audit est une formalité, et non une menace. »

5 Ratio d'efficacité du programme

Ce que ça mesure :

le retour sur investissement pur et dur. Combien d'euros économisés pour chaque euro dépensé en sensibilisation. Le Saint Graal des métriques business.

Pourquoi c'est important :

c'est LE chiffre qu'ils comprennent tous instantanément. « 1 € investi = 3,80 € économisés ». Pas besoin d'explications complexes, c'est le langage universel du business.

Comment la calculer :

1. **Prenez votre chiffre total annuel de coût des incidents évités (de la métrique 2).**

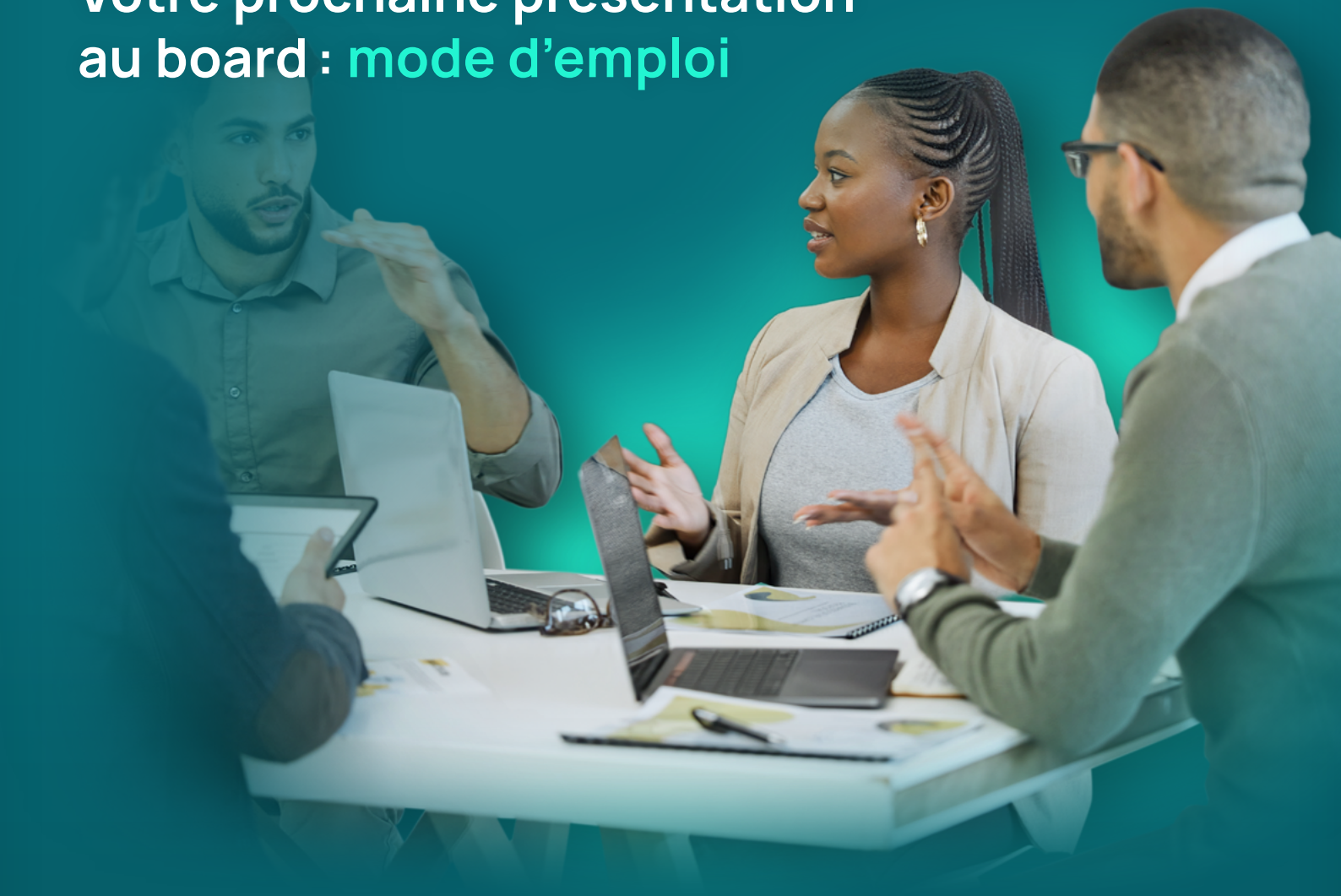
2. **Divisez par le coût total de votre programme de sensibilisation pour la même période.**

3. **Présentez comme « X € retournés pour 1 € dépensé. »Exemple :** pour chaque 1 € investi, 3,80 € de pertes potentielles ont été évitées l'année dernière.

Message pour le board :

« Notre programme de sensibilisation est l'investissement cybersécurité le plus rentable. Meilleur ROI que n'importe quel outil technique. »

Votre prochaine présentation au board : mode d'emploi



Ces cinq métriques transforment votre programme de sensibilisation en investissement rentable et mesurable. Désormais, vous présentez des euros économisés, des risques évités et un ROI prouvé, pas des taux de participation.

Pour commencer : établissez vos métriques de référence dès aujourd'hui. Documentez chaque incident évité. Quantifiez chaque gain. Les données feront le reste.

Votre programme devient ainsi un actif stratégique qui protège l'entreprise tout en générant un retour sur investissement démontrable.

Vous souhaitez adapter ces métriques à votre contexte spécifique ?

Parlons-en pour rendre le ROI visible dans votre stratégie de sensibilisation

Parler à un expert SoSafe