SENSIBILISATION À LA SÉCURITÉ DE L'INFORMATION

Où en sont les entreprises françaises ?

Benchmark 2015

Contact :
Michel Gérard
michel.gerard@conscio-technologies.com
+33 (0)6 07 04 92 57

Contact :
Gérôme Billois
gerome.billois@solucom.fr
+33 (0)6 10 99 00 60

UN ENJEU

« Mesurer dans la durée l'efficacité de la sensibilisation à la sécurité de l'information »

Priorisation des actions de sensibilisation

Reporting au management

Amélioration continue

Janvier 2016 - Propriété de Solucom, reproduction interdite

LE PANEL D'ENTREPRISES EN 2015

La plus large étude menée en France

12 entreprises
ayant déjà mené des démarches de sensibilisation

70 000 collaborateurs

28 000 répondants

Janvier 2016 - Propriété de Solucom, reproduction interdite

UN OUTIL

ISAM (Information Security Assessment Maturity) de Conscio Technologies

30 questions selon 11 thèmes

3 niveaux d'évaluation

Fort (> 80%)

Moyen (entre 70% et 80%)

Faible (< 70%)

3 axes d'appropriation de la cybersécurité

Sensibilité

Connaissance

Comportement

Janvier 2016 - Propriété de Solucom, reproduction interdite

DES QUESTIONS A CHOIX MULTIPLES

Vous êtes amené à travailler dans un immeuble à contrôle d'accès par badge. Une personne arrive avec les bras chargés et vous demande de lui ouvrir la porte. Que faites-vous ?

- Vous appelez un agent de sécurité afin que celui-ci vienne l'aider
- Vous lui indiquez l'agent d'accueil pour qu'il vérifie son identité et lui ouvre la porte
- Vous lui prenez les documents des bras afin qu'elle puisse sortir son badge
- Vous lui ouvrez immédiatement la porte, la pile de documents semble lourde

COMPORTEMENT

Vous souhaitez envoyer un document par e-mail ou bien l'imprimer. Comment traiter cette information au regard de sa confidentialité ?

- Il y a bien une politique de classification mais elle est difficile à comprendre
- La politique de classification est claire et bien expliquée dans l'entreprise
- Pas besoin de se préoccuper de cela, il n'y a aucune information confidentielle dans l'entreprise
- Vous vous fiez à votre jugement, c'est à chacun de savoir ce qui est confidentiel ou non au regard du métier de l'entreprise

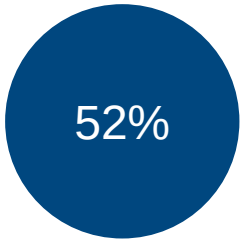
SENSIBILITE

+

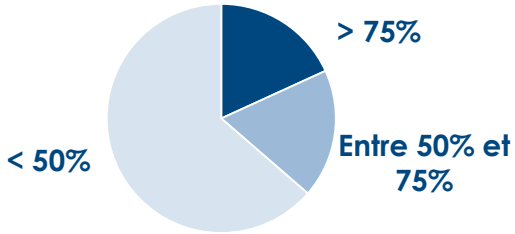
CONNAISSANCE

Janvier 2016 - Propriété de Solucom, reproduction interdite

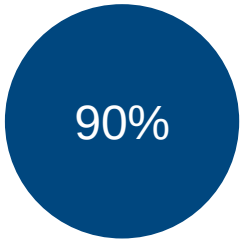
CONSTAT #1 : LES QUIZZ, CA MARCHE !



Taux de participation moyen sur le panel



Répartition des taux de participation selon les entreprises du panel



Taux de réponses à l'ensemble des questions

Facteurs d'explication des disparités au sein du panel :

- Importance de la communication autour de l'évènement
- Niveau de relance pendant la durée de la campagne
- Période de l'année à laquelle la réalisation du parcours a eu lieu (surcharge d'activité, vacances, etc.)
- Culture de départ de l'entreprise : plus la culture est établie, plus la participation à ce type de campagne est forte

Janvier 2016 - Propriété de Solucom, reproduction interdite

CONSTAT #2 : LE CHANGEMENT DES COMPORTEMENTS EST UN LONG CHEMIN

82%

Score moyen sur l'axe
« sensibilité »

Perception que les collaborateurs ont des risques de sécurité de l'information liés à leur comportement

75%

Score moyen sur l'axe
« connaissance »

Niveau de connaissance des collaborateurs sur les enjeux et les bonnes pratiques de sécurité de l'information

73%

Score moyen sur l'axe
« comportement »

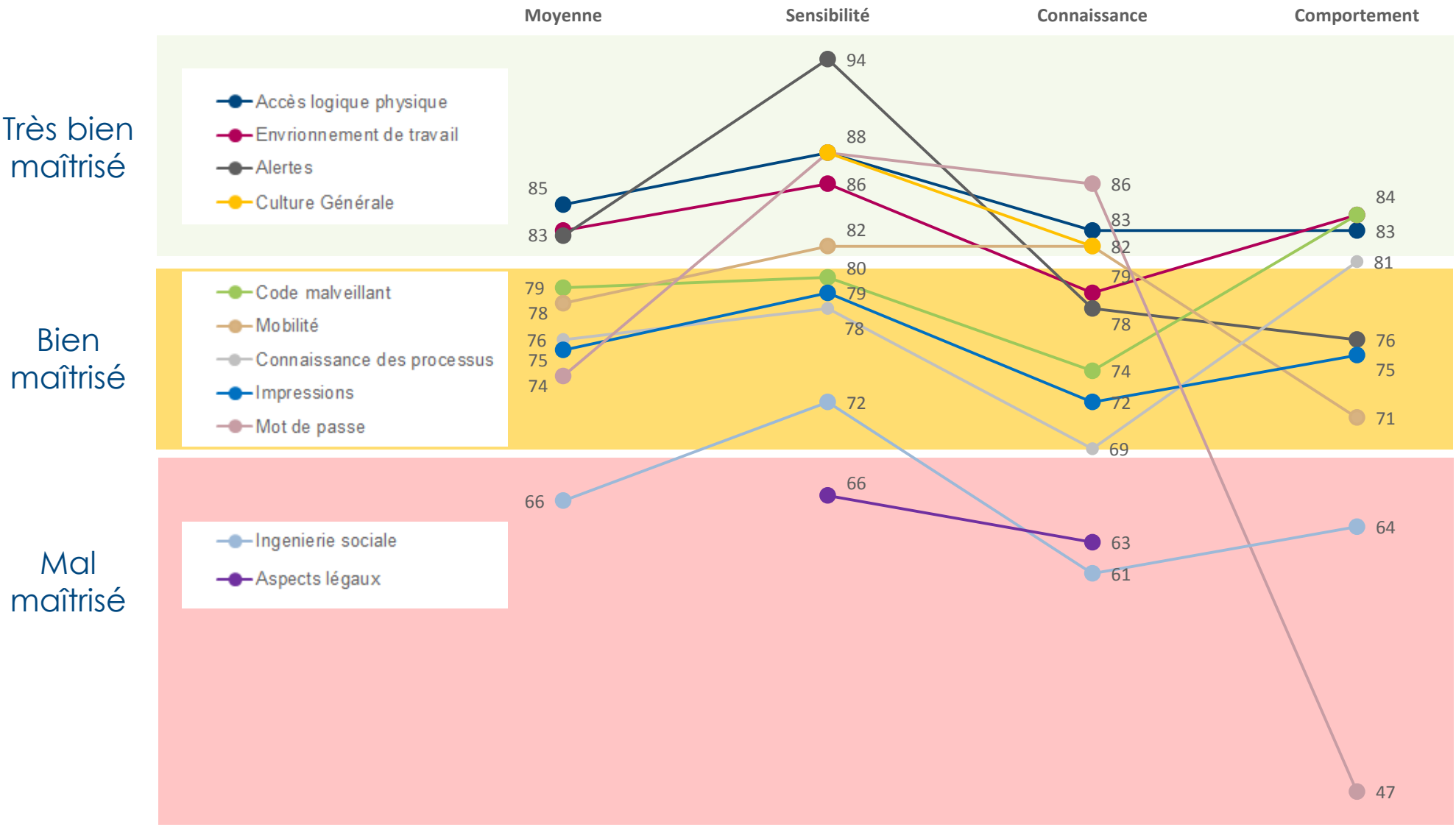
Niveau de respect, par les collaborateurs, des comportements attendus

La grande majorité des répondants est effectivement sensibilisée aux enjeux de sécurité.

Cette prise de conscience des enjeux doit conduire à terme à un changement des comportements. Néanmoins, les effets sur le comportement ne se traduisent pas encore, les collaborateurs ne mettent pas toujours en œuvre toutes les bonnes pratiques de sécurité.

Janvier 2016 - Propriété de Solucom, reproduction interdite

LES RÉSULTATS DÉTAILLÉS

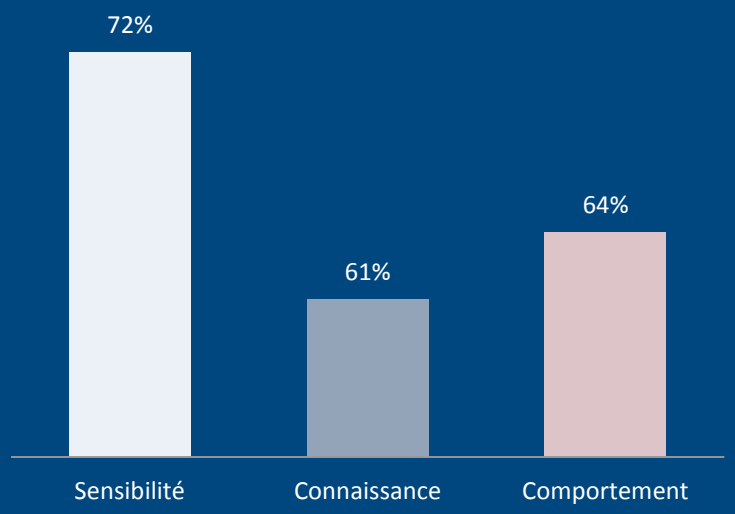


Janvier 2016 - Propriété de Solucom, reproduction interdite

LES PRINCIPAUX ENSEIGNEMENTS

Ingénierie sociale

LA priorité de 2016



L'ingénierie sociale (envoi de faux mails, appels frauduleux, etc.) constitue une porte d'entrée importante sur le SI de l'entreprise.

Or, les collaborateurs manquent de connaissance sur la conduite à tenir en cas de réception d'un mail de phishing ou lors de la connexion à un site Internet qui demande de fournir ses identifiants.

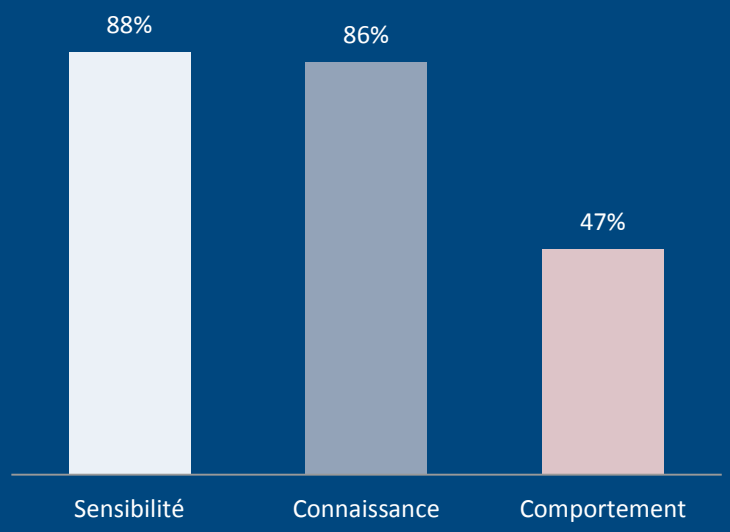
Au vu de l'augmentation et de la sophistication de ce type d'attaques, la prévention contre l'ingénierie sociale doit être une priorité

Janvier 2016 - Propriété de Solucom, reproduction interdite

LES PRINCIPAUX ENSEIGNEMENTS

Mots de passe

Il faut outiller !



La gestion des mots de passe est un thème privilégié de toute campagne de sensibilisation depuis des années.

Malgré une bonne connaissance des enjeux, les collaborateurs ne mettent pas en œuvre les pratiques de protection des mots de passe.

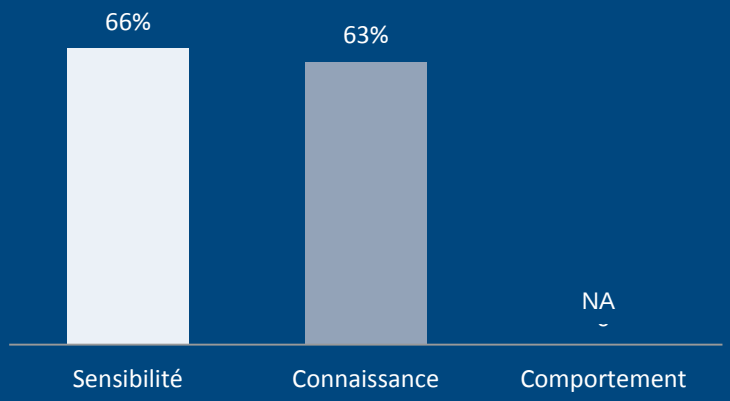
Le RSSI doit se rendre à l'évidence, seuls des projets techniques de protection des moyens d'authentification permettront de sécuriser les accès logiques.

Janvier 2016 - Propriété de Solucom, reproduction interdite

LES PRINCIPAUX ENSEIGNEMENTS

Aspects légaux

Les risques légaux sont mal connus



Les collaborateurs n'ont pas conscience que leur responsabilité est engagée lorsqu'ils prêtent leur mot de passe ou l'accès à leur messagerie à un collègue.

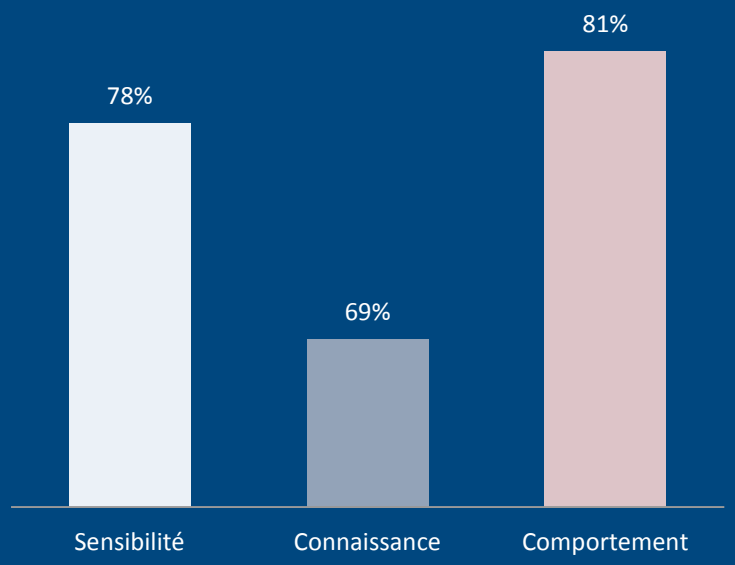
Les connaissances sur la protection des données à caractère personnel sont faibles ; ce point doit être renforcé, en particulier dans le contexte de déploiement du règlement européen *(General Data Protection Regulation)*.

Janvier 2016 - Propriété de Solucom, reproduction interdite

LES PRINCIPAUX ENSEIGNEMENTS

Connaissance des processus

La fonction RSSI doit mieux se faire connaître



Les collaborateurs sont sensibles à la prise en compte de certains documents de sécurité (charte, politique de sécurité) et adoptent le bon comportement.

Néanmoins, ils disposent d'une connaissance faible sur les documents clés et sur les interlocuteurs de la filière SSI qui sont mal identifiés et qu'ils ne savent pas joindre.

Le niveau de connaissance des processus de déclaration d'alertes et d'incidents de sécurité est également à améliorer.

Janvier 2016 - Propriété de Solucom, reproduction interdite

CONCLUSION

- Aucune entreprise du panel n'a atteint le niveau fort, alors qu'elles sont déjà engagées depuis plusieurs années dans le développement de la culture sécurité
- Un élargissement du panel pourrait conduire à la mise en évidence d'un niveau de sensibilisation moindre
- Néanmoins, on constate que le travail de prise de conscience des enjeux commence à porter ses fruits

RENDEZ VOUS L'ANNÉE PROCHAINE POUR LE SUIVI DES TENDANCES !

Janvier 2016 - Propriété de Solucom, reproduction interdite

Conscio Technologies est spécialiste de la sensibilisation à la sécurité de l'information et aux problématiques internes d'entreprise.

Conscio Technologies édite les solutions SaaS RapidAwareness et Sensiwave.

Basées sur les normes réglementaires et les politiques internes, ces solutions permettent de gérer en toute simplicité des campagnes de communication en ligne innovantes. Les programmes de sensibilisation à la sécurité informatique sont conçus pour répondre aux besoins d'organisations de toute taille et de tout secteur d'activité.

Solucom est un cabinet de conseil fondé en 1990. Sa vocation ? Guider et réussir les transformations d'entreprise. Une mission que le cabinet poursuit avec la conviction que la clé des transformations réussies réside dans la maîtrise simultanée de leurs enjeux business, organisationnels et technologiques. Les clients de Solucom sont dans le top 200 des grandes entreprises et administrations.

Début janvier 2016, Solucom s'est rapproché des activités européennes de Kurt Salmon (hors retail et consumer goods) donnant ainsi naissance à un nouveau leader du conseil en Europe.

Janvier 2016 - Propriété de Solucom, reproduction interdite