CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Organisation et sensibilisation : un duo gagnant pour le RSSI ?

Un pas vers l'homo securitus ☺

Eric Wiatrowski
Chief Security Officer
Orange Business Services

orange™

Quelle est la place du RSSI dans une entreprise ?

- Un alibi pour l'entreprise face aux tiers ou en cas de coup de tabac ?
- Un poil à gratter salutaire pour identifier les risques et convaincre de la nécessaire remédiation ?
- La mouche du coche qui complique la vie des salariés et embourbe le business ?
- Le responsable sur qui l'on tape le jour où ?
- Le superman qui solutionne tout problème de sécurité ?

Un homme (*)
parmi
Les hommes
(*)

Une petite parenthèse sémantique

- L'appellation consacrée de Responsable de la Sécurité du Système d'Information, ou de Responsable de la Sécurité laisse poindre un préjugé.
- Nos amis anglo-saxon ont choisi Chief Security Officer (CSO) ou Chief Information Security Officer (CISO) qui range la fonction dans la grande famille des CEO, CFO, CIO…
- On passe ainsi de responsable à patron, leader… chef d'orchestre
- A vous de comprendre le signifié dans votre entreprise.

Quel sont les facteurs humains qui contribuent à la sécurité ?

- Les décideurs : Comité de Direction et assimilables
  - Ils arbitrent les priorités
  - Ils sont comptables des ressources de l'entreprise
  - Ils sont légalement responsables des décisions de l'entreprise

- Les opérationnels : les acteurs terrain
  - Entre la chaise et le clavier
  - Toute APT commence par un mail, pdf, fichier Excel…
  - Un élément clé du dispositif opérationnel de sécurité

Acte 1 : Comment mobiliser les décideurs?

- Utiliser la peur, *dura lex*, *sed lex* ?
- Expliquer que la sécurité est une affaire d'experts ?
- Montrer la dernière étude de Machin Inc. Group qui évalue chaque incident de sécurité à 853,95 USD ?
- Démontrer un RoI positif pour les CAPEX et OPEX sécurité ?
- Construire le risk register ?

- Leur faire faire ce qu'il aiment : décider

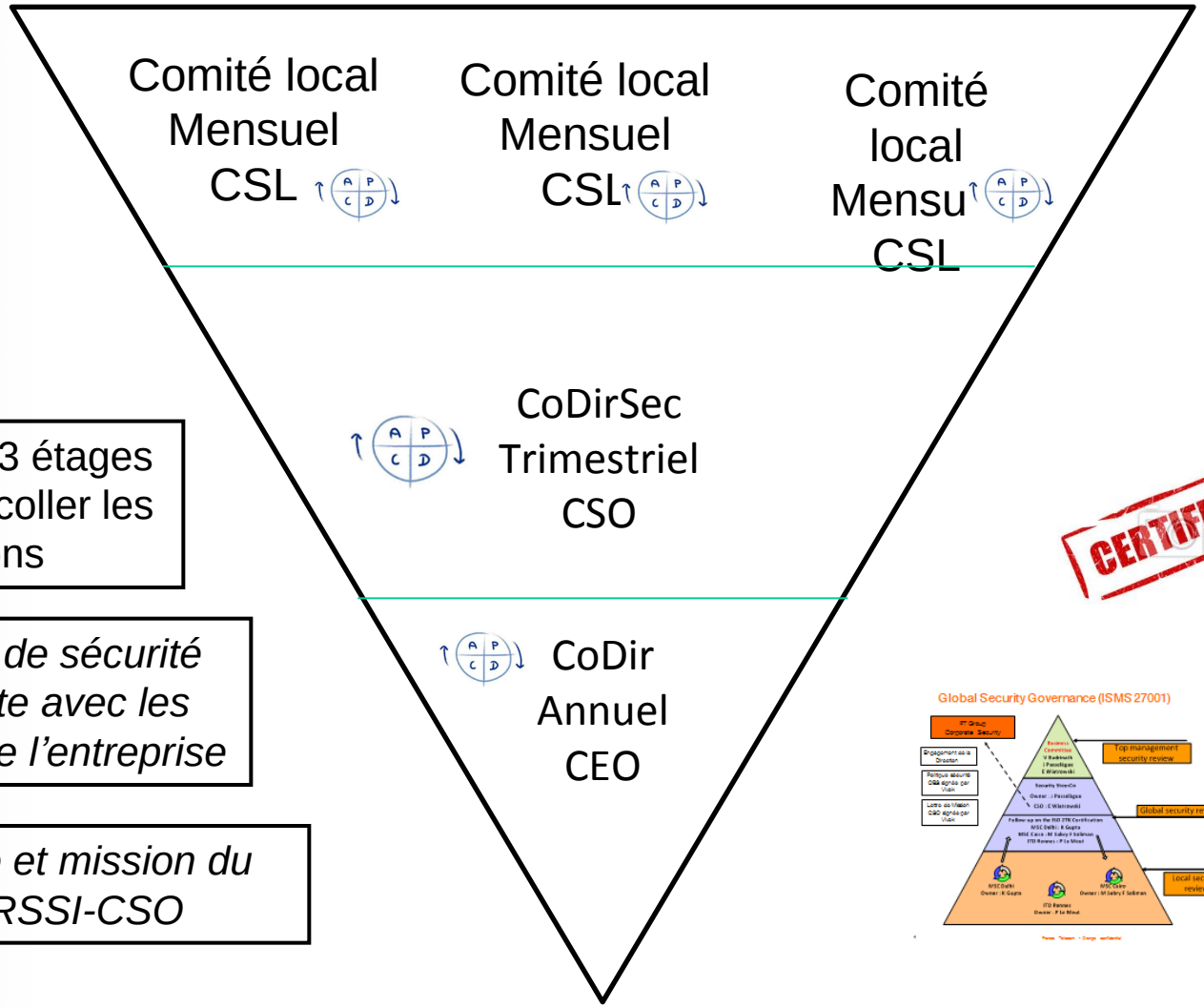
Mettre en place une gouvernance globale de la sécurité – la stratégie

- Elle doit être indépendante de l'organisation qui change au gré des acquisitions, fusions, optimisations…
- Ne pas se focaliser sur le rattachement hiérarchique du RSSI
- Construire une gouvernance fonctionnelle de la sécurité
- Ne pas exiger trop du Comité de Direction
  - Revue annuelle a minima
  - Intervention sur sujet critique au cas par cas
- Mettre en place un Comité de Direction Sécurité (CoDirSec)
  - Intronisé comme un sous-comité du CoDir
  - Sous responsabilité d'un membre du CoDir
  - Chaque membre du CoDir mandate un ou plusieurs représentants au CoDirSec
  - Il gère le SMSI global de l'entreprise

Mettre en place une gouvernance locale de la sécurité – l'opérationnel

- Dans chaque entité représentative de l'organisation mettre en place une entité locale de gestion de la sécurité
- Nommer un point de contact sécurité qui anime un réseau
  - Un Correspondant Sécurité Local
  - Un réseau de Correspondants Sécurité si nécessaire
  - Le CSL gère le SMSI local
    - Production des KPI sécurité
    - Gestion locale des incidents
    - Revue de management (analyse de risques)

Un schéma possible pour la gouvernance sécurité



Une fusée à 3 étages pour faire décoller les décisions

Politique de sécurité cohérente avec les objectifs de l'entreprise

Rôle et mission du RSSI-CSO

Acte 2 : La sensibilisation des utilisateurs

- Toute APT passe par un peu d'ingénierie sociale (cas RSA) et l'action d'un utilisateur : ouverture d'un mail, lancement d'un fichier Excel, connexion à un site Web, branchement d'une clé USB…
- La sensibilisation permet de réduire la surface d'attaque
- Même si certains pensent que c'est peine perdue et qu'il faut verrouiller l'Internet, bloquer les pièces jointes, résiner les ports USB…
- Remarque : un utilisateur bien formé peut valoir tous les IDS du monde : « j'ai reçu un mail d'un collègue en vacances », « un site institutionnel semble avoir changé de comportement », « je reçois un ordre du DG en franglais »…

Quelques pistes pour la sensibilisation

- Les posters dans les couloirs
- Le site intranet avec une vignette sécurité
- La campagne de mailing, avec un émetteur bien choisi qui incitera à lire le mail
- Les vidéos du commerce ou faite « maison »
- Les interventions dans les comités de direction
- La présentation en amphi avec une tête d'affiche type le DG-CEO ou la DCRI (très convaincante)
- Les jeux de rôles (scènes de théâtre)
- Semer des clés USB « piégées » dans les parkings et dans les halls
- Franchir le Rubicon des certifications pour certains acteurs : Risk Manager, Lead Auditor, CISSP…

Quelques conseils

- La sensibilisation doit être récurrente : on oublie vite les règles d'hygiène (ANSSI)
- Elle doit être soutenue, relayée par le management (exemplaire)
- Elle doit être parfois généraliste (tous publics) et parfois ciblée sur une population
  - « Finance » face aux arnaques mail ou téléphone
  - « Support en ligne » pour usurper un mot de passe utilisateur
  - « MOA SI » sur les bonnes règles de codage (SANS institute)
- Mesurer l'appropriation par des enquêtes et questionnaires
  - Simples et peu exigeants en temps de réponse
  - Analyser les réponses ET le taux de retour
- Le RSSI/CSO est le Chef d'orchestre de la sensibilisation

Exemple de questionnaire

Merci de bien vouloir répondre à cette interview.

- Pour votre activité, la Sécurité de l'Information c'est
  - Très important
  - Moyennement important
  - Pas important
  - Je ne me sens pas concerné
- Quels sont les gestes qui font partie de vos habitudes en termes de sécurité?
  - Je ne transmets pas mes ID/PW à mes collègues
  - Je marque mes documents bureautiques 'interne' ou 'confidentiel'
  - Je porte mon badge visible
  - Je maîtrise les informations que je transmets à mes partenaires externes
  - Je n'ouvre pas les mails d'origine ou de contenu douteux
  - J'évite d'utiliser les clés USB de tiers
- Savez-vous ce qu'est l'ingénierie sociale ?
  - L'art de manipuler des personnes pour atteindre un objectif sans que celles-ci ne s'en rendent compte
  - Construire ensemble un réseau social
- Quel service associé à la PKI utilisez-vous ?
  - Authentification et ouverture de session du PC
  - Signature et chiffrement des messages
  - Chiffrement du disque dur

Conclusion

- Le RSSI : Responsable ou Chef d'orchestre ?
- Le RSSI : dans la stratégie ou dans l'opérationnel ?

- Rappel : Une certification ISO 27001 exige l'implication démontrée de la Direction et des actions de sensibilisation

merci