

Plan de l'intervention

A adapter selon la problématique de votre entreprise

Introduction : définition de la cybercriminalité
définition des termes techniques utilisés

◆ **Risques identifiés et solutions proposées :**

● 12 études de cas (dont chaque dirigeant pourra choisir les thèmes qui l'intéresse)

- Le comportement à risques du salarié
- La fraude financière via la comptabilité
- La divulgation de savoir faire
- Le téléchargement illicite et l'intrusion via le réseau sans fil
- la défaillance de la sauvegarde des données
- le vol d'ordinateur portable ou de PDA (téléphone portable intelligent).
- le sabotage interne d'une base de données
- le dysfonctionnement ou l'altération des données par des programmes malveillants
- la diffamation (par courrier électronique, réseaux sociaux ou autre)
- la défiguration de site internet
- les bootnets
- le cybersquatting

● Les 5 réflexes à avoir lors de la réception de courriers électroniques

● Les 5 réflexes à avoir lors de la connexion à un réseau WIFI

◆ **Risques supplémentaires identifiés**

- déni de service
- carence du fournisseur
- risques environnementaux
- erreurs et omissions
- non conformité réglementaire
- suivi lacunaire du matériel en fin de vie

◆ **Recommandation des institutions**

◆ **Conclusion :** Impact et occurrence des risques en entreprise.

Plan de l'intervention

A adapter selon la problématique de votre entreprise

Introduction : Définition de la cybercriminalité

◆ Déterminer ce que font les enfants et les adolescents sur Internet :

- Les 7 actions les plus réalisées par les moins de 16 ans.

◆ Internet et ses dangers :

- Répercussions sur la santé :
 - Le danger d'accoutumance.
 - Les symptômes psychologiques.
 - Les symptômes physiques.
 - Internet : ça se soigne !
- L'insécurité :
 - Les données privées.
 - Les virus – les vers – les chevaux de Troie.
 - Le phishing.
 - La manipulation psychologique.
 - Le recrutement des sectes.
 - La diffamation sur Internet.
 - Les contacts dangereux.

◆ Le problème particulier de la cyber-pédophilie :

- Profil psychologique du pédophile.
- Profil psychologique des victimes.
- Mode opératoire du cyber-pédophile :
 - Mode d'approche de la victime.
 - Sélection de la victime.
 - Evaluation des risques.
 - Mise en place du premier contact.
- Repérer si le mineur est victime d'un cyber-prédateur.

◆ Répercussions pénales :

- La surveillance des salariés : est-ce légal ?
- Aspects juridiques :
 - La responsabilité civile et pénale des parents.
 - Les achats en ligne.
 - Comment signaler un site à caractère pédophile.

Conclusion : conseils psychologiques

- Informations pour une navigation tranquille, selon les âges.