Protection des données

Formation en 2 jours

et maîtrise de l'information stratégique en entreprise

Gestion maîtrisée des risques liés à l'information sensible en entreprise

Actualité de la question

Sous la pression d'un contexte sécuritaire international et celui de la lutte contre une cybercriminalité croissante, d'une part, et celle les enjeux sociétaux, économiques et financiers, d'autre part, et face aux exigences d'un management judiciarisé, l'entreprise doit appréhender les méthodes et les outils d'intelligence économique et gérer la sécurité globale de ses informations sensibles et stratégiques.

Pédagogie

Active et participative, travail sur cas.

Objectifs de la formation

- Assimiler le concept d'intelligence économique pour une mise en œuvre efficace contre la cybercriminalité.
- Initier un dispositif de veille simple
- Identifier et de localiser le patrimoine informationnel
- Agir sur le facteur humain pour améliorer la sécurité de l'information
- Modifier des éléments organisationnels de l'entreprise pour réduire les vulnérabilités informationnelles
- Maîtriser les outils informatiques et numériques vecteurs de pertes informationnelles importantes
- Identifier les forces et les faiblesses du Web et des réseaux sociaux dans la gestion informationnelle
- Préparer la participation à un salon professionnel en garantissant la sécurité de l'information stratégique.

Public concerné

Tout public, direction, chargé de sécurité, chef de projet.

Programme

Premier jour

I. Protéger le patrimoine informationnel

- **Le concept d'intelligence économique :** étude des besoins, organisation et acteurs de la politique interne, règles déontologiques.
- **La technique de veille :** collecte, traitement et diffusion de l'information (méthodologie et outils).
- **Le patrimoine informationnel enjeu de l'intelligence économique :** principes généraux de protection de l'information contre la cybercriminalité, en France et à l'étranger, rôle et processus d'intelligence économique, protection des données (méthodologie et outils).
- **Le facteur humain :** technique de renseignement humain. Méthodes d'acquisition (intrusion, écoute, fouille), identifier les acteurs potentiellement vulnérables (concurrents, stagiaires, consultants, prestataires…).

II. Cas concret

Deuxième jour

III. Optimiser l'organisation et la gestion des risques liés au patrimoine informationnel

- **Optimiser l'organisation de l'entreprise :** management spécialisé, sensibilisation des personnels, gestion des visiteurs, moyens dédiés.
- **Optimiser la gestion des outils informatiques :** stratégie de sécurité de l'information, risques numériques et parades, identifier les vulnérabilités.
- **Se protéger contre les actes de cybercriminalité :** Web et réseaux sociaux, fonctionnement du web 2.0, éducation des comportements individuels, publication compulsive et utilisation des réseaux.
- **Participation à un salon professionnel :** politique globale de sécurité nécessaire à la protection de l'information lors de la participation à un salon professionnel (anticipation, actions défensives et offensives, débriefing…).

IV. Étude de cas

V. Conclusion

Organisation du stage

Encadrement pédagogique

Un expert en protection de l'information stratégique, issu de l'IERSE (actuel INHESJ)

Documentation

- Un dossier pratique
- Le dernier numéro de la revue *Préventique*

Durée et horaires

- 2 jours, durée adaptable à vos besoins

Cette formation en intra-entreprise

Cette formation organisée sur mesure, spécialement pour votre structure, à l'intérieur ou non de vos locaux.

Cette solution présente **plusieurs avantages** :

- **financier**, puisque son principe est basé sur un coût fixe prépondérant et peu de frais variables, ce qui entraîne des économies d'échelle dès lors que vous êtes en mesure de mobiliser un minimum de 3 ou 4 personnes ; elle réduit également les frais liés aux déplacements des participants ;
- au niveau des **ressources humaines**, elle offre la possibilité de viser un objectif complémentaire de motivation d'équipe ;
- de **planning**, vous choisissez les dates de votre formation.

Cette solution permet :

- **d'adapter le contenu théorique** à votre contexte et le modifier en fonction de vos attentes ;
- **d'élaborer des travaux pratiques sur mesure** et recueillir parfois les témoignages d'un ou plusieurs acteurs ou témoin, disponibles sur place, et invités par le formateur.

Bulletin d'inscription

Protection des données et maîtrise de l'information stratégique en entreprise

☐ **Nous sommes intéressés par une session en intra-entreprise, concernant ___ personnes, merci de prendre contact avec nous.**

Nom : _____

Prénom : _____

Société / Organisme : _____

Fonction / Service : _____

Adresse : _____

Code postal : _____ Ville : _____ Pays : _____

Téléphone : _____ Télécopie : _____

Courriel (obligatoire) : _____ @ _____

Date : **Signature :**

Préventique – 6 rue du Courant – 33310 Lormont – www.preventique.org
Service formation – Tél. : 05 56 79 10 55 – Fax : 05 57 87 45 64 – Courriel : formation@preventique.org
Organisme de formation enregistré sous le n°72 33 06924 33 auprès du préfet de la région Aquitaine
Règlement par chèque bancaire ou postal à l'ordre du Groupe Préventique - RIB 10907 00001 92021393796 83 - Banque Populaire du Sud-Ouest