

Cyber-risques : prévention, protection et assurance - PCT15

Code produit : PCT15

Niveau : Expertise

Modalité : Presentiel

Durée (en heure) : 7.0

Tarif : 462,00 € HT

Eligible DDA : oui

Public :

Dirigeants, managers et collaborateurs

Prérequis :

Aucun

Objectif

- Maîtriser la cartographie des risques numériques
- Être capable de proposer la mise en place de mesures de prévention contre les risques cyber
- Pouvoir anticiper les évolutions réglementaires du marché de l'assurance cyber

Programme de la formation

1. Rappel des principes généraux de l'assurance cyber
 - Garanties d'un contrat cyber
2. La cartographie des risques cyber au travers d'exemples survenus récemment

- Statistiques sinistres cyber : focus sur les causes liées à des défaillances humaines
 - Activités les plus exposées
 - Analyse des principaux risques : malwares et virus / ransomware, attaques sur DNS ou DOS, phishing, doxing / ransomware, vandalisme pur
 - Cyber-risques : quelles conséquences envisageables sur les organisations ? Cartographie et analyse des risques au travers d'exemples récents
 - Schéma de présentation et d'analyse de chacun des risques cartographiés
3. Le télétravail : une nouvelle source de vulnérabilité aux risques cyber
- Contexte et risques
4. Tour d'horizon des principaux modes de prévention et de protection aux risques cyber
- Méthodes de prévention : antivirus, firewall, sondes, ingénierie sociale, contrôle des accès / politiques des mots de passe...
 - Focus sur les tests de résistance des SI
 - Méthodes de protection pour minimiser la portée du sinistre : sauvegardes, mirroring, formation des équipes d'intervention, expert en forensique, plan de continuité/reprise d'activité, communication interne, communication avec les tiers lésés, communication institutionnelle (risque de réputation)
5. Perspectives : l'évolution du marché de l'assurance cyber
- Pression des réassureurs
 - Mises en garde des pouvoirs publics
 - Attrition des garanties et des capacités
 - Assurabilité à terme
 - Solutions alternatives de gestion du risque cyber

Moyens d'évaluation

- Evaluation des acquis de la formation par le biais de QCM et/ou d'exercices pratiques
- Questionnaire de satisfaction à chaud complété par chacun à l'issue du stage
- Questionnaire d'évaluation à froid complété par chacun entre 2 et 3 mois après le stage

Méthodes pédagogiques

- Exposés à partir d'un diaporama
- Échanges d'expériences
- Réalisation de cas pratiques

AF2A - 64 Rue de Miromesnil, 75008 Paris

Copyright 2024 AF2A. Tous droits réservés.