

L'ARGUS

de l'assurance

■ ■ ■ Formations

CLASSE VIRTUELLE - CONNAÎTRE LES SOLUTIONS D'ASSURANCE CYBER RISQUES

Quelles offres proposer aux entreprises pour répondre à leurs enjeux business et obligations réglementaires

3 X 1H10, DE 18H00 À 19H10

DDA

CODE : ADIW01

Objectifs de la formation

- Identifier les risques et impacts du cyber pour l'entreprise
- Proposer une offre de cyber risque répondant aux besoins des entreprises
- Sensibiliser les entreprises à la nécessité d'une cyber assurance

Animée par

- AGHROUM Christian
Fondateur et gérant,
SOCOA

Public concernés

Le marché du cyber risque : contexte et enjeux

Évolution et environnement du cyber risque

- Les risques de la carte de paiement sans contact
- Le système européen SEPA : quels changements ?
- Le développement de la réalité augmentée et de l'Affichage Tête Haute
- L'émergence du « Hack As A Service »

- Courtiers; Agents généraux; Mandataires; Responsables et Chargés de clientèle au sein des organismes d'assurance; Souscripteurs et Rédacteurs; Gestionnaires de contrats d'assurance, Conseillers commerciaux en gestion de patrimoine

Dates

- Classe virtuelle
20-23/10/2020

Prérequis

- Cette formation entre dans le champ d'application des dispositions relatives à la formation professionnelle continue car considérée comme une action d'adaptation et de développement des compétences des salariés.

Modalités pédagogiques

- Tous nos stages de formations sont limités, dans la mesure du possible, à une douzaine de participants.
- Les formations se déroulent en présentiel ou en classe virtuelle avec un équilibre théorie / pratique. Chaque fois que cela est pertinent des études de cas et des mises en pratique ou en situation sont proposées aux stagiaires.
- Un questionnaire préalable dit 'questionnaire pédagogique' est envoyé aux participants pour recueillir leurs besoins et attentes spécifiques. Il est transmis aux intervenant(e)s avant la formation, leur permettant de s'adapter aux publics.
- Toute formation se clôture par une évaluation à chaud de la satisfaction du stagiaire sur le déroulement, l'organisation et les activités pédagogiques de la formation. Les intervenant(e)s évaluent également la session.
- Une auto-évaluation des acquis pré et post formation est effectuée en ligne afin de permettre à chaque participant de mesurer sa progression à l'issue de la formation.
- Une évaluation à froid systématique sera effectuée à 6 mois et 12 mois pour s'assurer de l'ancrage des acquis et du transfert de compétences en situation professionnelle, soit par téléphone soit par questionnaire en ligne.

- L'action de groupe : quelles conséquences ?

Du cyber crime au cyber terrorisme : quelles sont les différentes catégories ? De quelles attaques protéger les entreprises ?

Risque d'intensité ou de fréquence : comment vous positionner par rapport aux entreprises ?

- Adapter votre réponse au marché des ETI

Appréhender le cadre législatif du cyber risque

Les concepts du droit informatique et des SI

Quelles sont les particularités du cyber risque ?

De nouveaux dispositifs à l'horizon

- L'émergence d'une réglementation européenne : quelles conséquences ?
- Loi de programmation militaire

Quelles responsabilités pour l'assureur ?

Tarifs

■ Tarif Pack 15 heures	245,00 €HT
■ Tarif général	395,00 €HT

Quels défis pour les professionnels de l'assurance ?

Recouvrir les coûts liés à une attaque cyber criminelle

Limitier l'impact de l'incident par un apport d'expertise

Sensibiliser et assurer un rôle de conseil auprès de vos clients

Instaurer une veille technologique sur l'évolution de la cyber criminalité

Quelles solutions proposer pour assurer un cyber-risque ?

Mettre en place une couverture du cyber risque

- Déterminer les dommages potentiels : pertes d'exploitation, reconstitution des données, frais de notifications
- Définir les termes de la responsabilité civile
- Quel périmètre pour les amendes de la CNIL ?

Quel partenariat mettre en place pour créer des solutions de services d'expertises