

## ASSURANCE CYBER RISQUES

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

1 JOUR, 7 HEURES

PRODUITS

CODE : ADI01

### Objectifs de la formation

- Identifier les risques digitaux et le cadre juridique associé
- Proposer une offre de cyber risque répondant aux besoins des entreprises
- Sensibiliser les entreprises à la nécessité d'une cyber assurance

### Parmi nos formateurs

- AGHROUM Christian  
Fondateur et gérant,  
SOCOA

### Public concernés

- Directions générales, directions du développement, directions techniques, directions des risques, directions marketing, directions juridiques, courtiers

### 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.

### Tarifs

- Tarif Session en classe virtuelle : 995,00 €HT
- Tarif Session en présentiel : 1 060,00 €HT

### Le marché du cyber risque : contexte et enjeux

Test de connaissances: quiz sur les impacts des cyberattaques

### Évolution permanente du cyber risque

- Le phénomène du Cloud computing et du Big Data
- BYOD et consomérisation : les risques liés aux nouveaux usages
- L' e-réputation des entreprises
- Les objets connectés, la réalité augmentée : vers de nouvelles cibles ?

### EXERCICE Exercice de mise en situation

- Au moyen d'un cas pratique fil rouge seront envisagés, tout le long de la journée l'ensemble des sujets essentiels et d'actualité en matière de cyber risque.

---

**EXERCICE** Exercice d'application : définir les critères d'assurabilité d'une entreprise face au cyber risque

---

Du cyber crime au cyber terrorisme : de quelles attaques protéger les entreprises ?

---

**EXERCICE** Exercice d'application : identifier les attraits que l'entreprise présente pour les cyber-criminels

---

L'émergence du « Crime As A Service »

---

De quelles attaques protéger les entreprises ?

- Cyber attaques : de la technique à l'ingénierie sociale
  - Les techniques d'ingénierie sociale
  - Le top 5 des cyberattaques
  - Focus sur ransomwares, fraudes au président, dénis de service ...
- 

**EXERCICE** Exercice d'application : identification des actions à mettre en œuvre pour réduire les cyber risques à travers un exercice d'hygiène informatique

- Partage d'expérience sur la sensibilisation des entreprises à la cybersécurité
- 

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

---

Les enjeux du cyber risque sur votre organisation

- Mesurer et prévoir les coûts financiers
  - Anticiper les sanctions juridiques
  - Apporter des réponses en termes de gestion de crise et de réputation pour les entreprises
  - Développer un savoir faire spécifique au marché
  - Adapter votre réponse au marché des ETI
- 

Partage d'expériences: échange sur les différentes clauses contractuelles ou sur la gestion des risques

---

**Appréhender le cadre législatif et normatif du cyber risque**

Les concepts du droit informatique et des SI

---

Quelles sont les particularités du cyber risque ?

---

Le RGPD, ses conséquences, l'action de classes

---

Loi de programmation militaire

---

Le poids et l'intérêt des normes

---

## Analyse de textes juridiques

- RGPD
- Loi de Programmation militaire

**ILLUSTRATION** Etude d'un organigramme des fonctions clé, présentation de systèmes de management de la sécurité, de management ISO, etc.

### Quels défis pour les professionnels de l'assurance ?

Quelles solutions proposer pour assurer un cyber-risque ?

Quelles responsabilités pour l'assureur ?

Recouvrir les coûts liés à une attaque cyber criminelle

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

Sensibiliser et assurer un rôle de conseil auprès de vos clients

Instaurer une veille sur l'évolution de la cyber criminalité

Les critères pour estimer l'assurabilité d'une entreprise au cyber risque

- Mesurer les conséquences d'une attaque
- Quelle interconnexion du système d'information avec l'extérieur ?

**EXERCICE** Exercice d'application : comment proposeriez-vous votre offre à une entreprise ?

### 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 ?

**ILLUSTRATION** Le partenariat public / privé et la place de l'assurance

**CAS PRATIQUE** Quel support utiliser pour conclure l'offre avec l'entreprise étudiée

## Dates

Classe virtuelle Paris

01/12/2023 01/12/2023

## Modalités pédagogiques, d'évaluation et techniques

### ■ Modalités pédagogiques:

Pour les formations synchrones-présentiel ou classes virtuelles (formations à distance, en direct), les stages sont limités, dans la mesure du possible, à une douzaine de participants, et cherchent à respecter un équilibre entre théorie et pratique. Chaque fois que cela est possible et pertinent, des études de cas, des mises en pratique ou en situation, des exercices sont proposées aux stagiaires, permettant ainsi de valider les acquis au cours de la formation. Les stagiaires peuvent interagir avec le formateur ou les autres participants tout au long de la formation, y compris sur les classes virtuelles durant lesquelles le formateur, comme en présentiel peut distribuer des documents tout au long de la formation via la plateforme. 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. Pour les formations en E-learning (formations à distance, asynchrones), le stagiaire peut suivre la formation à son rythme, quand il le souhaite. L'expérience alterne des vidéos de contenu et des activités pédagogiques de type quizz permettant de tester et de valider ses acquis tout au long du parcours. Des fiches mémos reprenant l'essentiel de la formation sont téléchargeables. La présence d'un forum de discussion permet un accompagnement pédagogique personnalisé. Un quizz de validation des acquis clôture chaque parcours. Enfin, le blended-learning est un parcours alternant présentiel, classes virtuelles et/ou e-learning.

### ■ Modalités d'évaluation:

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. La validation des acquis se fait en contrôle continu tout au long des parcours, via les exercices proposés. Sur certaines formations, une validation formelle des acquis peut se faire via un examen ou un QCM en fin de parcours. 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.

### ■ Modalités techniques FOAD:

Les parcours sont accessibles depuis un simple lien web, envoyé par Email aux stagiaires. L'accès au module de E-learning se fait via la plateforme 360Learning. La durée d'accès au module se déclenche à partir de la réception de l'invitation de connexion. L'accès aux classes virtuelles se fait via la plateforme Teams. Le(a) stagiaire reçoit une invitation en amont de la session lui permettant de se connecter via un lien. Pour une bonne utilisation des fonctionnalités multimédia, vous devez disposer d'un poste informatique équipé d'une carte son et d'un dispositif vous permettant d'écouter du son (enceintes ou casque). En ce qui concerne la classe virtuelle, d'un microphone (éventuellement intégré au casque audio ou à la webcam), et éventuellement d'une webcam qui permettra aux autres participants et au formateur de vous voir. En cas de difficulté technique, le(a) stagiaire pourra contacter la hotline au 01 70 72 25 81, entre 9h et 17h ou par mail au [logistiqueformations@infopro-digital.com](mailto:logistiqueformations@infopro-digital.com) et la prise en compte de la demande se fera dans les 48h.