BLF

www.blf.education

L'ASSURANCE DES RISQUES CYBER

CYB_7h_1J

1 jour (7h)

PUBLIC

Tout intermédiaire d'assurance, collaborateur travaillant sur le marché des professionnels : chargé de clientèle Entreprise, chargé de compte, gestionnaire sinistres, etc.

PRÉREQUIS

Aucun

OBJECTIFS OPÉRATIONNELS

Dans le cadre de la distribution de produits d'assurance :
1) Sensibilisation aux risques Cyber
2) Connaitre les enjeux liés aux risques Cyber
3) Comprendre les garanties des contrats d'assurance Cyber en vue de présenter les offres d'assurance correspondantes.

FORMATEUR

Expert en Cyber risques ayant travaillé à la fois dans l'assurance et dans l'informatique

CONSULTEZ NOTRE PROCÉDURE D'ACCUEIL DES PERSONNES EN SITUATION DE HANDICAP

PROGRAMME

ÉLIGIBLE DDA

1) La cartographie des risques cyber
- Statistiques des sinistres cyber
- Analyse des principaux risques Cyber
- Conséquences sur les organisations
- Retours d'expériences au travers de cas réels
  - Fait générateur
  - Analyse des causes
  - Conséquences sur les organisations ciblées
  - Réponses apportées à l'incident
  - Enseignements
- Le risque Cyber et le Cloud

2) Le risque Cyber et la réglementation
- Les principaux organismes en charge du suivi réglementaire (CNIL, ANSSI…)
- RGPD
- Loi de Confiance en l'Economie Numérique

3) Focus sur les organisations des plus exposées
- OIV et OSE
- Commerce en ligne
- Entreprises stockant des données complexes ou dont la réalisation nécessite un investissement important
- SSII
- Secteur sanitaire et social
- Organisations utilisant des données sensibles
- Robotique (SCADA)
- Autres organisations

4) Principes généraux de l'assurance cyber
- Garanties du contrat cyber
- Définition des risques assurés
- Dommages garantis
- Dommages hors champ des cyber-risques
- Garanties optionnelles : fraudes, violation du protocole PCI-DSS et fraudes téléphoniques,

5) Principaux modes de prévention et de protection aux risques cyber
- Moyens de prévention : antivirus, firewall, sondes, ingénierie sociale (sensibilisation à la sécurité des SI, formation aux bonnes pratiques), contrôle des accès / politiques des mots de passe…
- Tests de résistance
- Test d'intrusion
- Scan des vulnérabilités
- Retours d'expériences
- Autres modes de protection/prévention : 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)

6) Le facteur humain principale cause des Cyber attaques
- Statistiques
- Les bonnes pratiques
- Focus sur le télétravail
  - Contexte du télétravail
  - Environnement informatique
  - Nomadisme
  - Mails frauduleux
  - Exemples de sinistres
- Les chartes de bonne conduite - formation

7) Perspectives : l'évolution du marché de l'assurance cyber
- La sinistralité
- L'évolution réglementaire
- Les conséquences de la dérive de la sinistralité sur l'assurabilité
- Solutions de management du risque cyber

Qualiopi processus certifié

RÉPUBLIQUE FRANÇAISE

MÉTHODES PÉDAGOGIQUES

- Exposés à partir d'un diaporama suivis de questions-réponses et d'échanges avec les participants
- Réalisation de cas pratiques, échanges d'expériences
- 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