Programmes courts

Gouvernance et cybersécurité

À Paris **Durée :** 1 jour **Tarifs :** public 1150€ net /adhérent 900€ net (frais de restauration inclus)

Depuis plusieurs années, plus une journée ou presque ne se passe sans qu'une entreprise « fasse la une » en raison d'une fuite d'informations digitalisées confidentielles. Dans ce contexte, cette formation vous aidera à mieux appréhender la complexité de ce risque (du fait de sa très forte dimension technique, de la multiplicité de ses conséquences, de son asymétrie, de son évolution permanente…) et en conséquence à mieux évaluer la pertinence des stratégies « cyber » déployées par les entreprises dont vous avez la supervision. Elle vous permettra également d'apprendre à mieux protéger les informations qui vous sont confiées.

Prérequis/Public visé

- Tout type d'administrateur(trice) souhaitant évaluer la gestion des risques de cybersécurité des entreprises supervisées et/ou souhaitant mieux protéger les informations qu'il/qu'elle détient.

Objectifs

- Connaitre les principaux risques « cyber » d'une organisation (sur la base de son activité, de son organisation, des réglementations applicables…)
- Savoir évaluer la pertinence des outils et méthodes mis en place par l'entreprise pour se défendre
- Connaître les principaux outils de protection disponibles pour la sécurisation des données détenues par les administrateurs.

Compétences visées

A l'issue de la formation le participant sera capable de :

- De maitriser l'essentiel du vocabulaire (complexe) de la cybersécurité
- D'identifier et d'évaluer les principaux risques « cyber » d'une organisation ainsi que leurs conséquences (opérationnelles, financières, juridiques…).
- D'évaluer la qualité et la quantité des moyens mis en œuvre par l'entreprise pour sa défense (au regard de ses risques)
- De mieux protéger les données détenues au titre des fonctions d'administrateur.

Programme

I/ Introduction

- Petit sondage interactif introductif : comment protégez-vous les données numériques qui vous sont confiées ?
- Quelques chiffres importants en matière de cybersécurité ;
- Quelques « mots clés » de la cybersécurité :
    - Sécurité de l'information vs sécurité de l'informatique
    - Présentation du concept de « surface d'attaque »
    - Le tryptique Confidentialité, Intégrité et Disponibilité
    - Le tryptique Identification, Authentification, Autorisation
    - Le chiffrement
    - Autres termes clés

II/ Les conséquences de la matérialisation des risques « cyber »

- Conséquences opérationnelles
- Conséquences financières
- Conséquences juridique (dans le cadre du RGPD, de NIS2…) - introduction au cadre juridique de la cybersécurité et de la protection des données personnelles
- Conséquences réputationnelles
- Conséquences humaines

III/ Identifier et évaluer les risques « cyber »

A/ Identifier simplement les risques « cyber » de son organisation

B/ Présentation des principales « failles » de sécurité de l'information

1) Les erreurs humaines
    - Les pertes matériel
    - Les mises à jour non réalisées
    - Les mots de passe faibles
    - Le phishing
    - La connexion à des réseaux non sécurisés/navigation sur internet/messages sur internet et réseaux sociaux
    - L'élicitation
    - Usage personnel et professionnel des matériels
    - Les logiciels freemiums et le « shadow IT »
2) Les attaques
    - Les attaques par phishing
    - Les attaques par dictionnaire et force brute
    - Les attaques par déni de service
    - Les attaques par dépassement de tampon
    - Les attaques web (manipulation d'URL, injection SQL, cross-site scripting…).
    - Les attaques « man in the middle".
    - La fraude au Président…

IV/ La gestion de la cybersécurité : les principaux livrables d'un programme de cybersécurité et le rôle de l'administrateur (pour chaque livrable, une checklist de vérification vous sera communiquée)

- La Gouvernance de la sécurité de l'information
- Le budget cybersécurité
- L'analyse des risques « cyber »
- La veille technique et réglementaire
- La PSSI et la charte informatique
- La cartographie des matériels et des données
- La gestion des accès (avec un focus sur l'Active Directory et les comptes d'administration)
- La gestion des mots de passe (et plus largement de l'authentification)
- L'analyse des vulnérabilités et la gestion des mises à jour
- Le chiffrement
- La gestion des programmes
- La formation des collaborateurs
- L'identification des failles de sécurité
- La gestion des incidents (y compris en cas de violation de données personnelles)
- La communication de crise
- L'assurance des risques « cyber »

V/ La « boite à outils » de l'administrateur pour protéger les informations qu'il détient dans le cadre de son mandat

- Gestionnaire de mots de passe
- VPN
- 2FA
- Outils de chiffrement (de document, d'espaces disque, des messages)
- Autres outils