EduGroupe
Accompagner pour réussir

Les enjeux de la cybersécurité dans son organisation - pour les dirigeants

Référence : **SECENJEUX**

Durée : **1 jour (10 heures) et 3 heures**

Certification : **Aucune**

Connaissances préalables

- Aucuns prérequis

Profil des stagiaires

- Dirigeants d'entreprise, Cadre d'entreprise, Responsable Informatique

Objectifs

- À l'issue de la formation, le stagiaire sera capable de s'approprier les enjeux et clés stratégiques de la sécurité numérique dans son organisation
- Plus précisément :
- Comprendre les enjeux stratégiques de la cybersécurité dans une organisation
- Situer la cybersécurité dans la gouvernance d'entreprise et adapter sa posture
- Connaître le cadre réglementaire et les obligations légales
- Favoriser une culture cyber dans l'entreprise

Certification préparée

- Aucune

Méthodes pédagogiques

- Présentations interactives avec échanges constants pour contextualiser les concepts et illustrer les enjeux,
- Études de cas réels, exercices en sous-groupes (salles virtuelles),
- Tableau blanc collaboratif,
- Sondages/quiz,
- Retours d'expérience,
- Trames et modèles opérationnels,
- Signature d'une feuille d'émargement pour attester de la présence à chaque demi-journée de formation.

Formateur

- Consultant-formateur expert en Cybersécurité

Méthodes d'évaluation des acquis

- Participation et réalisation d'exercices tout au long de la formation
- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestations des compétences acquises et de fin de stage adressée à chaque participant

EduGroupe
Accompagner pour réussir

Contenu du cours

1. Mesurer le risque numérique (1/2 journée – 3 h 30)

- Introduction : Recueil des attentes et règles de fonctionnement
- Comprendre son activité numérique : Transformation numérique et nouvelles dépendances ; valeur métier et biens supports ; cartographier le SI et l'écosystème (partenaires, fournisseurs, cloud).
- Le risque numérique : êtes vous une cible ? Économie de la malveillance ; valeur de la donnée ; attaque directe vs contagion ; supply chain, usurpation, fraude.
- Les grands types de menace : Tactiques/techniques/procédures d'attaque ; vulnérabilités et chemins d'attaque ; événements redoutés.
- À quels impacts s'attendre ? Impacts processus, opérationnels/physiques, financiers, réputationnels, juridiques ; dynamique choc/souffle/répliques.
- Construire ses scénarios de risque et définir son seuil d'acceptation : Identification d'événements redoutés et scénarios critiques ; estimation sommaire de la vraisemblance et de l'impact ; définition du seuil d'acceptation et options de traitement (réduire, transférer, accepter).
- 💡 *Livrables & travaux : méthode + cadre d'étude du risque remis ; étude d'un risque.*

2. S'organiser et piloter (1/2 journée – 3 h 30)

- Introduction : Retour sur l'étude de risque du processus critique sélectionné ; responsabilité du dirigeant
- Définir un cadre de gouvernance du risque numérique (amélioration continue) : Rôle RSSI / référent cyber / conseillers ; PSSI ; obligations et référentiels (NIS2, RGPD…)
- Développer une culture de sécurité numérique : Placer l'humain au centre ; former et sensibiliser les collaborateurs (rituels, KPI d'acculturation)
- Définir sa stratégie de sécurité numérique : Objectifs de sécurité basés sur les risques ; choix du référentiel ; arbitrage sécurité vs résilience
- Mettre en place des polices d'assurance adaptées : Pourquoi assurer le risque cyber ? Choisir sa police ; articulation avec le contrôle interne
- 💡 *Livrables & travaux : plan de PSSI + référentiels d'objectifs remis ; PSSI – chapitre « Objectifs » à produire*

3. Bâtir sa sécurité numérique et la valoriser (1/2 journée – 3 h 30)

- Introduction : Retour sur les PSSI ; cadrage des objectifs de la demi-journée
- Bâtir sa protection : Parcours progressif de sécurisation (du diagnostic initial à la conformité) ; choix des mesures de sécurité
- Orienter sa défense : Veille (menaces/vulnérabilités) : acteurs, solutions, intégration dans la posture ; anticipation : PCA/PRA
- Faire preuve de résilience en cas de cyberattaque : Gestion de crise : cellule, rôles et dynamique ; relations avec ACYMA, ANSSI, CERT/CSIRT, autorités, assureurs ; recours aux prestataires (PASSI, PAMS, PDIS, PRIS) ; entraînements/exercices
- Homologuer ses services numériques critiques : Référentiels de certification/homologation ; engagement raisonné du dirigeant
- Valoriser ses investissements en sécurité numérique : ROI : quantification financière du risque ; preuves de confiance dans la chaîne de valeur
- 💡 *Livrables & travaux : référentiel de conformité NIS2 remis ; positionnement initial et stratégie NIS2*

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.