Objectifs

- Mesurer le risque numérique
- Identifier les risques majeurs pour l'entreprise et les actions prioritaires à mettre en place
- Répondre aux exigences en termes de sécurité numérique
- Réagir en cas de crise cyber

Public concerné et prérequis

Dirigeants d'entreprise de taille moyenne ou de taille intermédiaire.
Membre du Comité Exécutif, Comité de direction.

Prérequis

Avoir réalisé le diagnostic de maturité cyber de l'entreprise avec l'outil 'MonAide Cyber' disponible via le lien suivant : https://monaide.cyber.gouv.fr

Qualification des intervenants

Spécialiste du domaine.

Moyens pédagogiques et techniques

Le module alternera éléments d'enseignement didactiques et théoriques avec une prise en main progressive des modules à travers des cas pratiques et des exemples exposant les principales problématiques que le stagiaire rencontrera dans la gestion du sujet de manière à acquérir une réelle autonomie opérationnelle.

Outils pédagogiques :
L'ensemble du cours est repris sous forme de projection par vidéoprojecteur.
Méthode affirmative ou magistrale (le formateur « dit »).
Méthode interrogative favorable aux échanges (le formateur « fait exprimer »).
Méthode démonstrative : démonstrations et exercices (le formateur « fait » et « fait faire »).
PC professionnel de l'apprenant et logiciel.
Vidéoprojecteur – ateliers de mise en pratique d'expérience.

Durée, effectifs

14 heures.

12 stagiaires.

Programme (contenu de la formation)

Jour 1

MISE EN SITUATION DE CRISE - SIMULATION - SERIOUS GAME

Introduction

Mise en situation

- Présentation du scénario de simulation (fictif mais inspiré de cas réels)
- Constitution des équipes / rôles (CEO, CISO, DRH, DAF, Communication...)
- Réalisation de l'exercice de gestion de crise

Retour d'expérience à chaud

- Bilan fictif : pertes estimées, impacts RH, image de marque, confiance
- Tour de table : ressentis, surprises, erreurs, réflexes

Apports pédagogiques

- Les spécificités de la gestion de crise cyber
- Les différents modes d'attaque et leurs impacts

MODULE 1 - MESURER LE RISQUE NUMERIQUE

Introduction

- Recueil des attentes des apprenants
- Règles et programme

Comprendre son activité numérique

- Transformation numérique et nouvelle dépendance
- Introduction du concept de valeur métier et de biens Ms
- Cartographier son système d'information et son écosystème

Le risque numérique : êtes-vous une cible ?

- La valeur de la donnée
- Attaque directe et contagion
- Les nouveaux champs de bataille

Les grands types de menace

- Notions de vulnérabilités et de chemins d'attaque
- Les motivations des attaquants
- Les événements redoutés

À quels impacts s'attendre ?

- Les différents impacts d'une attaque cyber (processus, gouvernance, physiques, financiers, réputationnels…)
- L'évolution des impacts (choc initial, souffle et répliques)

Construire ses scénarios de risque et définir son seuil d'acceptation

- Identifier les événements redoutés et quantifier leur vraisemblance
- Identifier les scénarios critiques d'attaques cyber
- Quantifier l'impact de ces scénarios et définir son seuil d'acceptation

Mis à disposition en fin de séance : méthodologie et cadre d'étude du risque numérique

Rendu à la fin de la période d'autonomie : étude d'un risque critique

Jour 2

MODULE 2 - S'ORGANISER ET PILOTER

Introduction

- Retour sur l'étude de risque du processus critique sélectionné
- Responsabilités du dirigeant

Définir un cadre de gouvernance du risque numérique (amélioration continue)

- Rôle des RSSI / référents cyber / conseillers cyber
- La politique de sécurité des systèmes d'information (PSSI)

Développer une culture de sécurité numérique

- Placer l'humain au centre du jeu
- Former ses collaborateurs

Définir sa stratégie de sécurité numérique

- Définition des objectifs de sécurité
- Choix du référentiel
- Priorité à la sécurité ou à la résilience ?

Mettre en place des polices d'assurance adaptées

- Pourquoi assurer le risque cyber ?
- Comment choisir sa police d'assurance ?

Mis à disposition en fin de séance : Plan d'une PSSI et référentiels d'objectifs de sécurité
Rendu à la fin de la période d'autonomie : PSSI (chapitre « Objectifs »)

MODULE 3 - BÂTIR SA SÉCURITÉ NUMÉRIQUE ET LA VALORISER

Introduction

- Retour sur les PSSI
- Cadrage des objectifs de la demi-journée

Bâtir sa protection

- Construction d'un parcours progressif de sécurisation (du diagnostic initial à la conformité)
- Le choix des mesures de sécurité

Orienter sa défense

- La veille (renseignement sur la menace et les vulnérabilités) : présentation des acteurs et solutions, intégration dans la posture de sécurité
- Anticiper sa réponse : les PRA et PCA

Faire preuve de résilience en cas de cyberattaque

- La cellule de crise : composantes et dynamique
- Les relations avec l'écosystème (ACYMA, ANSSI, CERT régionaux ou sectoriels, CSIRT, autorités, assureurs)
- Le recours à des prestataires (PASSI, PAMS, PDIS, PRIS)
- L'entraînement et les exercices

Homologuer ses services numériques critiques

- Les référentiels de certification et d'homologation
- L'homologation, une expression de l'engagement raisonné du dirigeant

Valoriser ses investissements en sécurité numérique

- Le retour sur investissement : quantification financière du risque cyber
- Le développement de la confiance numérique : les preuves de confiance

Mis à disposition en fin de séance : référentiel de conformité NIS2

Rendu à la fin de la période d'autonomie : positionnement initial et stratégie de conformité (NIS2)

Modalités d'évaluation des acquis

Chaque stagiaire devra effectuer un test de connaissance sous la forme d'un questionnaire oral et écrit avec le formateur reprenant les principaux points de la formation.

Sanction visée

Certificat de réalisation.

Matériel nécessaire pour suivre la formation

L'apprenant aura à sa disposition le matériel informatique professionnel.

Conditions de déroulement

Formation en INTRA - Formation en présentiel.
Alternance d'apports de connaissances théoriques, puis mise en pratique.

Délais moyens pour accéder à la formation

La planification de votre formation sera finalisée et inscrite à notre calendrier selon vos disponibilités et contraintes.

Accessibilité aux personnes en situation de handicap

Lors de l'inscription à nos formations, nous étudions avec le candidat en situation de handicap et à travers un questionnaire les actions que nous pouvons mettre en place pour favoriser son apprentissage. Pour cela, nous pouvons également nous appuyer sur un réseau de partenaires nationaux préalablement identifiés.

Taux de réussite à la formation

Taux de satisfaction de la formation

Tarif

Nous consulter.