FORMATION

Programme de Formation

Cybersécurité pour cadres dirigeants (banque & assurance)

Organisation

Durée : 7 heures

Mode d'organisation : Présentiel

Contenu pédagogique

Public visé

Membres de COMEX et de Conseils d'administration du secteur bancaire et assurantiel.

Directeurs généraux, directeurs financiers, directeurs des risques, directeurs de l'innovation.

Responsables de la conformité et de l'audit interne.

Toute fonction de direction impliquée dans la gouvernance et la gestion des risques.

Objectifs pédagogiques

- Donner une compréhension claire et opérationnelle des principaux risques cyber dans le secteur bancaire et assurantiel en 2025.
- Expliquer les enjeux réglementaires européens et français (DORA, NIS2, RGPD, LPM, AI Act).
- Sensibiliser au rôle du COMEX/Conseil d'administration dans la gouvernance et la gestion de crise.
- Illustrer les impacts de l'IA en cybersécurité, tant comme menace que comme outil de défense.
- Développer une capacité à prendre des décisions éclairées face aux incidents et à poser les bonnes questions aux équipes techniques.

Description

Introduction (30 min)

1. Panorama de la menace cyber (2h)

1.1 Haut du spectre (menaces stratégiques et systémiques)

États et groupes sponsorisés : cyberespionnage, déstabilisation, attaques sur infrastructures critiques

Risques systémiques : attaques coordonnées contre les systèmes de paiement, risques pour la stabilité financière

Cas récents (SWIFT, attaques DDoS sur banques, APT sur données clients et fusions-acquisitions)

1.2 Bas du spectre (menaces opérationnelles et criminelles)

Ransomwares et extorsion de données

Fraudes financières (phishing, vishing, BEC, deepfakes vocaux)

Marchés noirs et services cybercriminels à la demande (ransomware-as-a-service)

Cas concrets dans banque/assurance

1.3 Menace interne et risques organisationnels
Administrateur malveillant et abus de privilèges
Fuites de données intentionnelles ou accidentelles
Shadow IT et Shadow AI : risques liés aux outils non validés par l'entreprise
Gestion des insiders (RH, juridique, technique) et exemples sectoriels

(Pause café)

2. Panorama des réglementations et obligations (1h30) 2.1 Cadre réglementaire européen et international
DORA (Digital Operational Resilience Act) : spécificités pour la finance
NIS2 : obligations pour les opérateurs de services essentiels, doublon ou recouvrement avec DORA ?
RGPD & ePrivacy : enjeux de la donnée sensible
Règlement IA (AI Act) : la nouvelle donne

2.2 Cadre français et sectoriel
ACPR, AMF, CNIL, ANSSI : rôles et attentes
Recommandations spécifiques au secteur financier et assurantiel

2.3 Exemple de programme de mise en conformité type
Cartographie des risques et classification des actifs
Gouvernance de la sécurité (RSSI, comités de crise, chaîne de responsabilité)
Tests, audits, plans de remédiation
Gestion de la sous-traitance et du cloud (due diligence, audits fournisseurs)

2.4 : La LPM 2024-2030
Le statut OIV / OSE et ses obligations spécifiques.
Les interactions entre LPM, NIS2 et DORA.
Les attentes de l'ANSSI et la posture à adopter au niveau COMEX.

(Déjeuner)

3. Focus sur l'IA et ses impacts en cybersécurité (1h30) 3.1 L'IA comme menace
Génération d'attaques plus sophistiquées (phishing, deepfakes, contournement de détection)
Automatisation des cyberattaques
Risques de dépendance aux modèles externes (fuites, biais, manipulation)

3.2 L'IA comme défense
Détection d'anomalies et comportements suspects
Automatisation de la gestion des incidents
Perspectives : SOC augmenté par l'IA, red teaming automatisé

3.3 Cas pratiques et scénarios

Exemple de fraude par deepfake vocal dans une banque

Comment une IA défensive pourrait détecter des comportements anormaux dans des transactions

4. Gouvernance, gestion de crise et rôle du cadre dirigeant (1h)

- Responsabilité des dirigeants et risque pénal/civil
- Rôle du COMEX/Conseil d'administration : pilotage des risques cyber
- Gestion de crise : simulation d'attaque et communication de crise (clients, médias, régulateurs)
- Relation avec les équipes techniques : comment poser les bonnes questions

5. Perspectives et enjeux stratégiques (45 min)

- Géopolitique et cybersécurité financière : tensions Chine/USA/Europe
- Cyber-assurance : évolutions et limites de la couverture assurantielle face aux ransomwares
- Résilience numérique et confiance client comme avantage concurrentiel
- Discussion ouverte : comment ces enjeux transforment le métier des dirigeants

Clôture (15 min)

- Synthèse des points clés
- Conseils pratiques pour le COMEX : que retenir, quelles priorités ?

Prérequis

Cette formation ne nécessite pas de Prérequis.

Modalités pédagogiques

Formation interactive et didactique : présentation théorique, cas pratiques, analyses de bonnes pratiques

Moyens et supports pédagogiques

Remise du support pédagogique aux stagiaires

Modalités d'évaluation et de suivi

Un questionnaire préalable ainsi qu'une auto-évaluation d'entrée sont envoyés aux participants en amont de la formation pour mesurer leur niveau de maîtrise et permettre au formateur d'adapter sa pédagogie

Signature d'un émargement par les participants et le formateur afin de justifier l'assiduité de chacun (émargement électronique)

Recueil à l'oral des besoins par le formateur au démarrage de la formation

Echange en fin de formation entre les participants et le formateur pour valider que la formation a bien répondue aux attentes des participants et que les objectifs pédagogiques ont été atteints

Un questionnaire d'évaluation (auto-évaluation sortie de formation) est envoyé aux participants pour mesurer l'acquisition des compétences à l'issue de la formation

Un formulaire de satisfaction est rempli par les participants à l'issue de la formation pour recueillir leurs satisfactions et mesurer la qualité de la formation assurée.

Une attestation est délivrée à l'issue de la formation