Comprendre et gérer une cybercrise : les fondamentaux

Date et durée

Code formation : ARI002FR
Durée : 2 jours
Nombre d'heures : 14 heures

Description

À l'ère où le cyber-risque est devenu une **menace existentielle,** il existe deux types d'organisations : celles qui ont été piratées et celles qui ne le savent pas encore. Cette formation s'adresse aux leaders qui comprennent que le **pilotage d'une cybercrise** est avant tout un enjeu humain, managérial et organisationnel, dépassant largement le seul périmètre informatique.
Sur 2 jours, ce programme intensif fournit les **fondamentaux organisationnels et stratégiques** essentiels pour réagir efficacement à une attaque majeure. Il est conçu pour vous permettre de prendre les bonnes décisions, avec les bons moyens, face à un événement critique. Vous apprendrez non seulement à anticiper les risques, mais surtout à structurer et **animer une cellule de crise** impliquant toutes les fonctions de l'organisme (direction, cœur de métier et supports).
À travers des exemples concrets, des exercices pratiques et une **mise en situation réaliste**, vous développerez une vision complète pour comprendre, préparer et gérer tout type de crise, en vous focalisant ensuite sur les spécificités d'un scénario de cybercrise (rançongiciel, fuite de données, déni de service). L'enjeu est vital : **assurer la qualité de service et la continuité d'activité**.

Objectifs

À l'issue de cette formation en gestion de crise, vous atteindrez les objectifs de compétences suivants :

- comprendre la nature exacte d'une crise, et distinguer clairement une cybercrise des autres types d'incidents ;
- relier les enjeux de la gestion de crise générale aux spécificités managériales et organisationnelles des cyber-attaques ;
- adopter la posture d'un gestionnaire de crise efficace : définir les responsabilités, anticiper la prise de décision et maîtriser sa communication ;
- appliquer les clés du pilotage d'une cybercrise : se préparer en amont, gérer l'incident en temps réel et établir un bilan post-crise ;
- vivre une cybercrise simulée : participer à un exercice immersif pour tester vos réactions et consolider vos réflexes de cellule de crise.

Points forts

- **Vision stratégique complète :** une formation qui permet d'acquérir les bases de la gestion de crise avant de se focaliser sur les spécificités du cyber-risque.
- **Approche interactive et concrète :** des interactions continuelles entre le formateur et les participants, basées sur des exemples réels et des exercices pratiques.

- **Mise en situation réaliste :** l'inclusion d'une mise en situation complète et d'un quizz pour ancrer immédiatement les apprentissages.
- **Expertise pratique :** une animation effectuée par un professionnel expérimenté ayant eu des expériences de gestion de crise vécues en interne et en externe.

Modalités d'évaluation

Quiz / QCM
Travaux Pratiques

Pré-requis

Suivre cette formation nécessite les prérequis suivants :

- **Rôle de pilotage et de décision :** il est indispensable que vous occupiez ou soyez destiné à occuper un rôle de pilotage d'une crise et d'une cybercrise au sein de votre organisation (ComEx, Codir, responsable de crise, RPCA, etc.).
- **Vision managériale :** une capacité à dépasser les aspects purement techniques d'une attaque pour vous concentrer sur les enjeux stratégiques, managériaux, organisationnels et de communication.
- **Connaissance des enjeux métier :** une familiarité avec les processus critiques de votre organisation et les impacts potentiels d'une indisponibilité, afin de tirer pleinement parti des études de cas et de la mise en situation.

Public

Cette formation s'adresse aux professionnels qui ont, ou auront, un rôle de pilotage et de décision lors d'un événement critique impliquant la sécurité des systèmes d'information. Le public inclut notamment :

- Les **responsables du Plan de Continuité d'Activité (RPCA)** et de la gestion de crise.
- Les **dirigeants et membres du Comité de Direction (ComEx, Codir)** susceptibles d'intégrer la cellule de crise.
- Les **directeurs des risques et les managers** ayant à gérer des crises complexes, y compris d'origine cyber.
- Les **managers de la DSI et des fonctions support** ou opérationnelles impliqués dans la réponse et la communication de crise.

Programme

Module 1 : anticiper les risques et structurer la préparation

- Les concepts fondamentaux de la gestion de crise : terminologie, enjeux et implications managériales.
- L'analyse des différents risques de cybercrise : ransomware, fuite de données, indisponibilité des systèmes et leurs impacts métier.
- La compréhension du rôle des facteurs humains et organisationnels dans la survenance et l'escalade des incidents.
- La définition et la mise en place des structures de crise : de l'équipe d'incident (technique) à la cellule de crise (stratégique).
- La préparation du socle documentaire : le Plan de Continuité d'Activité (PCA) et le Plan de Gestion de Crise (PGC).

Module 2 : gérer la crise et renforcer l'organisation

- La gestion tactique d'une cybercrise : détection, confinement, communication et remédiation.

- La prise de décision en environnement incertain : les outils d'aide à la décision et les matrices de priorisation des actions.
- La communication de crise : gestion des parties prenantes (internes, externes, médias, régulateurs) et la protection de la réputation.

Travaux pratiques & cloture

- Mise en situation : appliquer les principes de gestion lors d'un scénario de crise réaliste et évolutif.
- Quiz de révision : valider vos acquis avec un test final.
- Conclusion : synthétiser vos acquis et élaborer un plan d'action personnel.