Communication de crise en cas d'attaque informatique

CYBERSÉCURITÉ

Objectifs	Apprendre à structurer et diffuser une communication efficace et adaptée lors d'une attaque informatique - Savoir gérer les relations avec les collaborateurs, la presse, les partenaires, et les autorités tout en maîtrisant les obligations légales - Anticiper les erreurs classiques et protéger l'image de l'organisation en situation critique.
Participants	Responsables communication - DSI - RSSI - membres de cellules de crise - juristes - responsables RH - dirigeants d'entreprise - consultants cybersécurité - gestionnaires d'incident - porte-paroles d'organisation.
Prérequis	Notions de cybersécurité basique - bonnes pratiques de communication - gestion de la réputation - capacité rédactionnelle - gestion du stress - relation avec les médias et parties prenantes.
Moyens pédagogiques	1 poste par participant - 1 vidéoprojecteur - Support de cours fourni à chaque participant - Ateliers Individuels - Modalités d'évaluation : Ateliers (TP) pendant tout le long de la formation et évaluation des acquis tout au long de la formation
Méthodes pédagogiques	Exposés interactifs et démonstrations - Travaux pratiques individuels et en groupe - Échanges d'expériences et de bonnes pratiques
Type de formation	Formation présentielle ou distancielle, selon les besoins et les contraintes des participants
Tarif inter-entreprise	4150 € HT
Durée	5 jour(s) – 35 heure(s)

Code : NCI_X8KQJM32

Programme :

Enjeux, acteurs et cadre légal

Principes de gestion de crise cyber

Risques réputationnels, psychologiques, juridiques

Obligations légales (RGPD, CNIL, ANSSI, autorités sectorielles)

Typologie des parties prenantes : internes, presse, clients, fournisseurs, CER

TP

Étude de cas : analyse d'un incident médiatisé (ransomware, fuites de données)

Cartographie des parties prenantes d'un cas d'école

Identification des obligations de notification (CNIL, ANSSI, clients…)

Construction des messages de crise

Règles d'or de la communication en crise : transparence, cohérence, rapidité

Construction d'un plan de communication : chronologie, porte-parole, canaux

Erreurs fréquentes à éviter (déni, flou, contradiction)

Communication interne vs externe : objectifs et contenu différenciés

Cas Pratique

Rédaction de communiqués de presse adaptés à différents publics (presse, salariés, partenaires)

Création de messages d'alerte (SMS, mail, push interne)

Simulation de briefs à destination des dirigeants (fiche réflexe)

Communication avec les autorités, clients et partenaires

Notifier un incident à la CNIL / autorités judiciaires / ANSSI / CSIRT sectoriel

Gérer les clients et partenaires sous stress (B2B/B2C)

Travailler avec un cabinet de communication de crise ou juridique

Gestion des demandes médias / journalistes / élus

Cas Pratique

Rédaction d'un mail type CNIL / ANSSI avec données pertinentes (fiche RGP, chronologie, mesures)

Construction d'une FAQ client pour incident de sécurité

Jeu de rôle : réponses à un journaliste, conférence de presse simulée

Simulation de cellule de crise et scénarios d'incident

Organisation d'une cellule de crise (rôles, canaux, rythmes)

Scénarios typiques : ransomware, fuites massives, sabotage interne, compromission cloud

Communication synchronisée avec l'IT et la direction

Cas Pratique

Simulation d'un incident cyber en temps réel

Attaque en cours, presse en alerte, données compromises

Préparation et diffusion des messages à chaud

Adaptation des messages selon l'évolution (fuite, pression médiatique, rançon)

Restitution et retour d'expérience

Scénario complet de gestion de crise cyber (attaque ciblée d'un groupe de menace connu)

Animation d'une cellule de crise communicante

Analyse post-incident : évaluation des messages, rapidité, coordination

Retour Exp : ce qui a marché, ce qui doit évoluer (méthodologie + posture)

WEDO 365 by NCI

Caen - Paris - Lyon - Rennes - Nantes - Le Havre - Nice - Montpellier - Lille - Toulon

Saint-Etienne - Toulouse - Montpellier - Bordeaux - Grenoble - Le Mans - Tours - Marseille

www.wedo365.fr - commercial@nci.fr - Tél : +33 (0)2 14 99 00 20