Exercices de gestion de crise cyber

Gestion de crise cyber

Trop souvent, la crise cyber reste un événement auquel on ne s'est pas préparé. Or le jour où elle se produit réellement, les équipes doivent faire face à une pression intense : informations partielles, décisions urgentes, coordination entre services, sollicitations médiatiques ou institutionnelles...

Un exercice de gestion de crise cyber permet de transformer un scenario catastrophe en une crise maitrisée. Il place les participants en situation immersive, avec un scénario crédible, une montée en tension progressive et des stimuli adaptés (emails suspects, fausses alertes techniques, appels de clients, rumeurs sur les réseaux sociaux...).

L'exercice au service de l'organisation

La pratique des exercices de gestion de crise cyber permet à l'organisation de:

- **Tester** ses procédures de réponse, de communication et de reprise d'activité
- **Identifier** les points de blocage humains et techniques
- **Renforcer** la capacité collective à agir sous pression
- **Ancrer** durablement les bons réflexes dans les équipes

Pourquoi en avez-vous besoin ?

- Pour créer un **levier de différenciation** : assurer vos clients et partenaires de vos capacités à assurer la continuité de vos activités dans le cas d'un acte de cyber malveillance
- Pour vous mettre en **conformité avec les réglementations** actuelles et à venir en matière de résilience des organisations.
- Pour **tester et améliorer la fiabilité** de votre plan de gestion de crise ou le construire
- Pour révéler les points faibles et les silences organisationnels. Ces révélations sont précieuses, car elles vous permettent de **corriger les problèmes** avant qu'une crise réelle ne survienne

La théorie vous prépare aux questions
L'exercice de crise vous prépare aux réponses.

Mettre les équipes en situation concrète de crise pour pratiquer et renforcer leur résilience

Une immersion collective réaliste et engageante pour :

- **Concrétiser le risque** : sortir la crise cyber de l'abstraction pour en faire une expérience vécue
- Simuler la pression de crise : exposer les équipes aux tensions (urgence, complexité, incertitude) et au stress
- **Mobiliser les compétences collectives** : communication entre services, prise de décision difficile, dilemme éthique
- **Développer les bons réflexes managériaux et opérationnels** : gérer des situations hors des cadres métiers habituels
- **Donner du sens à la préparation** : faire du cyber un sujet partagé entre les fonctions, les métiers, l'IT et la direction
- **Construire une feuille de route réaliste** : identifier des leviers de progrès tangibles (organisationnels, humains et techniques)

Approche

Exercice de crise du PCA : de la théorie à la résilience collective

Bien plus qu'une simple simulation technique, c'est un moment stratégique pour tester les procédures, l'efficacité de votre Plan de Continuité d'Activités et la réactivité de vos équipes.

En personnalisant le scénario, **nous préparons votre organisation** aux situations les plus défavorables, renforçant ainsi **la résilience de vos entités** dans un cadre réaliste.

CQFD a développé une méthode et un cadre structurés (référentiels, responsabilités, reporting) pour répondre aux enjeux de :

- Conformité : garantir le respect des exigences de NIS2, DORA, ISO/IEC 27001
- Organisation : mobiliser rapidement l'ensemble des équipes pour minimiser les impacts d'une cyberattaque
- Management : former les décideurs à agir vite, à communiquer clairement et à arbitrer sous pression
- Culture : créer un réflexe collectif et durable

Conformité

Organisation

Management

Culture

Au-delà de l'objectif de conformité
Un véritable levier de transformation pour votre organisation

Accompagnement complet

- Diagnostic de maturité de gestion de crise cyber
- Préparation technique et organisationnelle
- Acculturation des équipes et renforcement des réflexes
- Plan de continuité et de reprise des activités
- Documentations et fiches reflexes
- Conformité légale et gouvernance de crise
- Communication de crise
- Plateforme de gestion de crise

Méthodologie

Inventaire et cadrage

- **Evaluation de maturité à la gestion de cyber crise** (référentiel ANSSI)
- **Etude de la documentation existante** (ex: plan de gestion de crise, fiches reflexes, référentiels ciblés type NIS2 ou DORA...)
- **Identification des principaux intervenants** pour élaborer le scénario personnalisé
- **Réunions de validation des objectifs** définissant les processus et les vulnérabilités à tester

Conception de l'exercice

- **Elaboration du scénario personnalisé :** production du chronogramme des événements et des stimuli
- **Finalisation** de la liste des participants et de la logistique

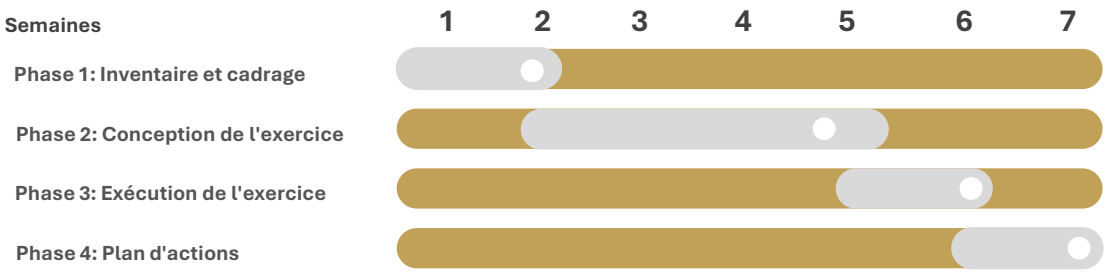
Exécution de l'exercice

- **Réunion de cadrage** avec les participants définissant les règles de l'exercice
- **Réalisation de l'exercice** avec un animateur et des stimulateurs en présentiel ou distanciel
- **Séance de compte rendu "à chaud"** sur les ressentis et la performance des participants

Plan d'actions

- **Débrief "à froid" avec les participants** identifiant les mesures correctives personnalisées
- **Rapport détaillé** décrivant les points forts et les points d'amélioration sur les cinq axes du diagnostic de maturité (gouvernance et coordination inter-équipes, détection et réponse à incident, continuité de service et reconstruction, communication de crise, processus et documentation existants)
- **Réunion de présentation des résultats** et des conclusions aux principaux intervenants
- **Evaluation maturité post-exercice**

Planning



Résultats et livrables

✓ Montée en maturité collective

Les équipes gagnent en réflexes, en confiance et en capacité d'action face à l'imprévu

✓ Amélioration des procédures

Les procédures existantes sont challengées, ajustées, clarifiées

✓ Renforcement de la coordination entre services

Les silos sont brisés, la coopération se fluidifie, les rôles et responsabilités deviennent plus lisibles

✓ Acculturation de l'ensemble de l'organisation

La cybersécurité devient un sujet partagé, compris, et intégré par tous

Livrables et matériel pédagogique

- Le kit de fiches réflexes « Les essentiels pour piloter une crise cyber »
- Des éléments de méthodologie pour la gestion de crise
- Le plan d'actions élaboré lors du débrief de l'exercice

- L'expérience d'une cyberattaque vécue et raconté par un utilisateur et un membre de la direction générale
Prix du Forum InCyber 2023

- Le livre blanc de l'ASSOVICA :
L'impact invisible des cyber malveillances

- Des vidéos témoignages de victimes de cyberattaques comme support de sensibilisation

La dimension managériale et humaine

Une gestion de crise efficace repose autant sur des procédures bien définies que sur des comportements adaptés. En situation réelle, la capacité à gérer le stress et à prendre des décisions rapides dans l'incertitude sont les deux facteurs qui déterminent la réussite.

L'approche de **CQFD** intègre pleinement cette réalité. Au-delà de la conformité, nous mobilisons les participants à travers une **expérience immersive** conçue pour simuler les **effets concrets** d'une crise : tension, pression médiatique, coordination interservices, saturation d'informations. Autant de situations où le stress est réel et où chaque décision compte.

L'objectif est clair : entraîner les équipes à réagir de manière structurée, lucide et collective, même dans le chaos.

La simulation constitue un levier pédagogique puissant, offrant aux participants une **expérience immersive et impactante**, bien plus efficace qu'un apprentissage purement théorique.

La simulation de crise cyber permet d'acquérir des **réflexes opérationnels durables**, de consolider la cohésion d'équipe et d'identifier les axes d'amélioration managériale souvent méconnus en situation normale.

En intégrant la dimension humaine comme élément central de l'exercice, cette méthode renforce la capacité des équipes à gérer avec efficacité des situations complexes ou inattendues. **Une approche pragmatique** pour développer l'agilité collective et anticiper les défis organisationnels.

Renforcez la posture de votre organisation face aux cybermenaces

L'exercice se concrétise par une dynamique d'action

- Décider en environnement incertain
- Prioriser, trancher vite en s'appuyant sur des faits incomplets et changeants
- Communiquer entre les services et avec le terrain
- Favoriser des échanges fluides entre IT, RH, direction juridique, communication, métier et éviter les silos
- Gérer le stress individuel et collectif
- Repérer les signaux faibles de désorganisation et mettre en place une régulation active
- Clarifier les rôles et responsabilités, savoir qui fait quoi, éviter les zones grises et les doubles décisions
- Agir en leader, faire émerger une posture de pilotage forte, collaborative et alignée sur les priorités

La dimension réglementaire et conformité

Transformer une obligation en levier de performance

La mise en conformité avec les réglementations européennes en matière de cybersécurité est aujourd'hui un impératif. Avec NIS2 (directive sur la sécurité des réseaux et systèmes d'information) et DORA (règlement sur la résilience opérationnelle numérique dans le secteur financier), les organisations sont désormais tenues d'adopter une posture active et démontrable en matière de gestion de crise cyber.
Cela implique notamment :

- La mise en place de plans d'intervention clairs en cas d'incident
- La réalisation régulière d'exercices de crise pour tester ces dispositifs
- L'implication des instances de gouvernance, y compris les conseils d'administration
- Un reporting structuré vers les autorités compétentes, dans les délais imposés

Un exercice de crise pour démontrer votre maturité

Conçu avec **les exigences des référentiels** en toile de fond, notre modèle d'exercice vous permet de :

- Tester vos capacités de détection, d'alerte, de réponse et de rétablissement
- Évaluer la coordination entre les directions techniques, juridiques et métiers
- Simuler les relations avec les régulateurs, clients ou médias
- Produire des éléments tangibles de conformité, valorisables en audit

En vous préparant activement, **vous renforcez votre résilience**, mais aussi votre crédibilité auprès de l'écosystème : clients, partenaires, autorités, assureurs...

Renforcez votre résilience et votre crédibilité auprès de l'écosystème

La simulation de crise représente un levier stratégique essentiel pour les organisations souhaitant maîtriser leurs enjeux de sécurité et de résilience.

Elle vous permet non seulement d'anticiper et de mieux piloter vos risques, mais aussi de formaliser et d'optimiser vos pratiques face aux incidents majeurs.

En renforçant votre préparation et votre réactivité, vous affirmez la maturité de votre organisation et consolidez votre position en tant qu'acteur de confiance dans l'écosystème numérique.

Standards cibles

- **NIS2**
- **Plan d'action CaRE**
- **DORA**
- **ISO/IEC 27001**
- **ISO 22301**
- **Référentiels de l'ANSSI**

Éric QUESSON
Fondateur
eric.quesson@cqfdsolutions.com
+33 6 69 51 20 23