Cybersécurité

Grille de Gestion de Crise

Pour Petites et Moyennes Entreprises

Soyez cyberfuté RBC®

rbc.com/cyberfute/entreprise

Préambule :

Comme la plupart des petites et moyennes entreprises (PME) ont de la difficulté à mettre en place des pratiques adéquates en matière de sécurité – que ce soit par manque de fonds ou de ressources – elles sont fréquemment la cible des cyberattaques. Souvent, un seul cyberévénement peut nuire à une PME et mener à des pertes financières et à une atteinte à la réputation, ou même à la dissolution de l'entreprise. Le présent document vise à contribuer à combler les lacunes quant à l'adoption de pratiques adéquates par les PME en matière de cybersécurité, en leur présentant les fondements d'une bonne gestion de crise, ainsi que les étapes pour se relever d'une cyberattaque.

Intervention : Planification de la gestion de crise

Nous envisageons la possibilité d'un **cyberévénement lorsque les systèmes d'information ou les actifs d'une entreprise sont exploités, altérés** ou **inaccessibles.** Il est essentiel que les PME aient un plan d'action structuré afin de répondre le plus efficacement possible. Afin de se préparer en vue d'un cyberévénement, les PME devraient élaborer une **norme de gestion de crise et un index des politiques à adopter en cas de cyberévénement,** en suivant les procédures décrites ci-dessous :

Fondements et politiques de planification préalable pour la gestion de crise

Classification des cyberévénements

Une entreprise peut uniquement gérer un cyberévénement si elle s'est adéquatement préparée. Les PME devraient établir quels événements peuvent avoir une incidence sur leur entreprise, ainsi que le niveau des dommages connexes subis. Le tableau ci-dessous donne un aperçu de la façon dont les cyberévénements sont classés ; il peut être personnalisé en fonction des cyberévénements uniques auxquels pourrait faire face l'entreprise qui met en place une norme de gestion de crise.

Exemples de types d'incident :

Indication d'un cyberévénement	Exemple	Procédure d'engagement	Niveau de gravité
Perte d'élément	L'employé perd son ordinateur portable ou son appareil mobile		Faible
Cible de mauvais pratiques en ligne	L'entreprise est la cible d'une campagne d'hameçonnage		Modéré
Panne de système	Panne des systèmes organisationnels (attaque par saturation)		Élevé
Violation de justificatifs d'accès	Les justificatifs d'accès d'un membre de la direction sont compromis, donnant ainsi accès à des renseignements sensibles.		Élevé
Incapacité d'accéder à des renseignements (rançongiciel)	Des renseignements organisationnels importants ne sont plus accessibles en raison de logiciels malveillants chiffrant les données.		Critique
Violation de données	Des renseignements et des registres de l'entreprise sont accessibles hors de l'entreprise.		Critique

Communication avec les parties prenantes

Une **partie prenante est une entité qui est visée par un événement, soit par l'incidence ou par le service offert.** La communication avec les parties prenantes est un aspect fondamental de la gestion de crise qui renforce la capacité d'une entreprise à faire face à un cyberévénement. La grille ci-dessous est conçue pour vous aider à repérer les parties prenantes au sein d'une entreprise afin de mieux établir qui est la bonne ressource et de réagir rapidement en cas de cyberévénement.

Parties prenantes liées aux TI :

Poste	Nom	Coordonnées de la personne-ressource principale	Service

Nota : Les parties prenantes liées aux TI doivent comprendre les personnes-ressources principales en matière de TI travaillant au sein de l'entreprise ou offrant des services à l'entreprise. (**Exemples :** Bureau de cybertechnologie, fournisseurs de services, service des TI, etc.)

Parties prenantes non-liées aux TI :

Rôle	Nom	Coordonnées de la personne-ressource principale	Service

Nota : Les parties prenantes non-liées aux TI sont des employés internes, des instances de gouvernance, des points de contact internes principaux, ainsi que des points de contact de tiers qui offrent un service à l'entreprise (**exemples :** Contentieux, Comptabilité, Ressources humaines, Affaires publiques, etc.)

Élaboration d'une procédure de mobilisation

La procédure de mobilisation est au cœur de toute grille de gestion de crise et présente en détail la façon dont l'entreprise souhaite gérer les cyberévénements d'une nature précise, en plus d'énoncer clairement les objectifs, la stratégie et la portée de la procédure. Les entreprises devraient s'appuyer sur les piliers de la procédure de mobilisation ci-dessous afin de mieux respecter les exigences d'une intervention adéquate en cas d'événement.

Énoncé de mission : Quel est l'objectif ?	**Exemple :** Atténuation des pertes de matériel de l'entreprise contenant des renseignements commerciaux (élément perdu)
Portée du plan : Quels sont les secteurs de l'entreprise touchés ?	**Exemple :** Secteur d'activité des employés et parties correspondantes.
Stratégie opérationnelle : Comment l'entreprise prévoit-elle reprendre le cours normal de ses activités ?	**Exemple :** – Désactivation temporaire de l'accès du compte de l'employé et demande de modification des justificatifs d'accès. – Gestion de la perte potentielle de renseignements conformément à la procédure et aux politiques sur la perte de données.
Communications : Comment gérons-nous les parties visées ?	**Exemple :** Respect des normes et des politiques en matière de communication aux parties concernées.

Nota : Les PME doivent prendre en compte les ressources dont elles disposent, leur fonction et leurs actifs afin d'élaborer un plan qui répond aux exigences uniques d'intervention à la suite d'un cyberévénement.

Grille de communication

Il est essentiel d'informer les parties visées, les parties prenantes et les principaux utilisateurs dans le cadre de la gestion de crise. Afin de mieux conseiller ces groupes, il est recommandé que les PME fournissent suffisamment de renseignements aux utilisateurs finaux sans divulguer tous les détails du cyberévénement avant qu'elles ne soient prêtes à communiquer tous les renseignements à cet égard, au besoin.

Déclaration générale :

- **Date et heure du jour**
- **Services touchés :** Quelles sont les fonctions de l'entreprise qui sont présentement touchées et non fonctionnelles
- **Nature de l'interruption :** Brève description de la cause
- **Heure et date du rétablissement du service :** Temps estimé pour rétablir les activités

Courriel général :

- **Priorité :** Faible, modérée, élevée, critique
- **Objet :** « Message à tous les employés : Alerte de sécurité – Crise (un sujet convenable exprimant l'urgence de la situation)
- **Corps du message :** Description de ce que les employés doivent faire ou de ce qu'ils doivent surveiller
- **Noms des personnes-ressources :** Coordonnées des instances de gouvernance, au besoin
- **Rappel concernant la protection des renseignements personnels, y compris les médias sociaux :** Rappel concernant la protection des renseignements personnels, annonce publique d'une entreprise faisant face à un cyberévénement peut entraîner des pertes monétaires ou une atteinte à la réputation.

Politiques de gestion de crise – Synthèse

En s’appuyant sur les grilles ci-dessus pour gérer les crises, les entreprises peuvent élaborer des politiques de gestion efficaces fondées sur :

- **Classification des cyberévénements :** Liste classant par ordre de priorité les cyberévénements possibles propres à l’entreprise.
- **Identification des principales parties prenantes :** Coordonnées des principales personnes-ressources, tant les techniciens que les non-techniciens, dans l’éventualité où il serait nécessaire de recourir à leurs services.
- **Procédure de mobilisation :** Plan de l’entreprise en cas de cyberévénement, indiquant comment les événements seront gérés et communiqués.
- **Grille de communication** : Grille de communication utilisée pour gérer les parties touchées.

Les PME doivent utiliser les documents ci-dessus quant à un cyberévénement pour répondre aux questions suivantes :

- **Que s’est-il passé ?**
- **Quelles sont les conséquences ?**
- **Quel est votre plan ?**
- **Comment communiquons-nous la situation ?**

Ces questions décrivent de façon globale chaque étape de gestion d’un cyberévénement, de la reconnaissance initiale à la résolution. Les personnes responsables de la création de la politique devraient adopter le point de vue de l’employé qui tente d’utiliser le plan de gestion de crise, afin de s’assurer que les exigences de la politique sont respectées. Vous trouverez ci-dessous un exemple de ces questions. Utilisées de concert avec les documents ci-dessus, elles peuvent contribuer à fournir un plan d’intervention efficace.

Exemple – Consignation d'une politique de gestion de crise

Gestion de crise – Perte d'un élément organisationnel *FAIBLE*

Parties prenantes liées aux TI

Poste	Nom	Coordonnées de la personne-ressource principale	Service
Gestionnaire d'accès	John Doe	555 555-1234	Gestion des droits d'accès
Responsable du provisionnement d'éléments	Jane Doe	555 555-9876	Provisionnement d'éléments

Parties prenantes non-liées aux TI

Poste	Nom	Coordonnées de la personne-ressource principale	Service
Expert-conseil en RH	Joan Doe	555 555-4334	Ressources humaines
Responsable des communications	Joanne Doe	555 555-2317	Communications
Secteur d'activité de l'employé	*Veuillez préciser*	*Veuillez préciser*	*Veuillez préciser*

Procédure d'engagement

Énoncé de mission :	Atténuation des pertes de matériel de l'entreprise contenant des renseignements commerciaux (élément perdu)
Portée du plan :	Secteur d'activité des employés et parties correspondantes.
Stratégie opérationnelle :	• – Désactivation temporaire de l'accès du compte de l'employé et demande de modification des justificatifs d'accès. • – Gestion de la perte potentielle de renseignements conformément à la procédure et aux politiques sur la perte de données.
Communications	Respect des normes et des politiques en matière de communication aux parties concernées.

Stratégie de communication :

Personnes-ressources **:** Gestion des droits d'accès, secteur d'activité de l'employé, parties visées

Norme de communication :

- **Priorité :** Faible
- **Objet :** « Message aux parties visées : Perte d'un élément »
- **Corps du message :** Un élément organisationnel a été signalé disparu ; veuillez suivre les normes de l'entreprise pour éviter d'autres pertes de données.
- **Noms des personnes-ressources :**
  - **Expert-conseil en RH :** Joan Doe – 555 555-4334
  - **Gestionnaire d'accès :** John Doe – 555 555-1234
- **Rappel concernant la protection des renseignements personnels, y compris les médias sociaux :** *Rappel concernant la protection des renseignements personnels*