

Les 48 premières heures : l'intervention après une violation de données

29 MAI 2017 1 MIN DE LECTURE

Expertises Connexes

- [Cybersécurité et intervention en cas d'incident lié à la sécurité](#)
- [Services professionnels](#)

Auteurs(trice): [Christopher Naudie](#), [Adam Kardash](#)

L'intervention initiale de votre organisation à la suite d'une atteinte à la sécurité des données est critique à la détermination de l'impact à long terme de l'incident sur votre entreprise. Les mesures immédiates que vous prenez après l'atteinte peuvent donner le ton à l'intervention et influencer sur la facilité avec laquelle votre organisation peut se remettre de l'événement.

En cas de violation de données : les 5 priorités

1



CIRCONScrire

Prendre immédiatement des mesures pour identifier et circonscrire l'incident

- Des mesures de TI
- Des mesures de sécurité
- Des mesures auprès du personnel

Former une équipe d'intervention

- Susciter l'engagement des équipes de protection de la vie privée, du service juridique, des communications et des ressources de TI
- Désigner un coordonnateur de l'intervention

Ne pas compromettre la capacité d'enquête

- Préserver les métadonnées et suivre la piste
- Conserver, séparer et préserver les documents sans les modifier
- Faire appel à des conseillers juridiques ou à une équipe d'enquête externe

2



ENQUÊTER

L'enquête préliminaire

- Faire appel à une équipe d'experts judiciaires
- Déterminer la cause et l'étendue de la violation - relève-t-elle de notre responsabilité?
- Maintenir une chaîne de possession de la preuve
- Établir des protocoles visant à protéger la confidentialité
- Cerner l'univers des personnes et des activités qui ont pu être touchées

Évaluer l'exposition Enquête judiciaire à long terme

3



COMMUNIQUER

Intervention immédiate

- Songer aux obligations de notification en vertu de la réglementation
- Déterminer s'il y a eu un RPPG - un « risque réel de préjudice grave »
- Communiquer avec votre personnel
- Établir une stratégie pour atténuer l'atteinte à la réputation
- Établir une stratégie pour les communications externes

Sensibilisation à long terme

4



AVISER

Aviser les organismes de réglementation

- Commissaires à la protection de la vie privée
- Police
- Organismes professionnels et autres organismes de réglementation

Aviser les particuliers

Aviser les parties intéressées

5



CORRIGER

Mesures correctives pour remédier aux préjudices subis par les parties

- Mesures de récupération des données
- Mesures pour empêcher leur diffusion et leur divulgation
- Possibilité de surveillance du crédit
- Évaluer s'il y a lieu d'offrir un dédommagement
- Prévoir une stratégie en cas de poursuite judiciaire, y compris un recours collectif

Pratiques exemplaires - les éléments clés d'un protocole d'intervention en cas d'incident

Les éléments clés de la préparation à une violation des données :

- L'établissement d'un protocole et d'une structure de reddition de comptes efficaces
- L'identification des fournisseurs de services et d'autres parties intéressées clés
- La mise en œuvre de mesures pour protéger la confidentialité
- La disponibilité de l'assurance
- La valeur de la vérification de l'état de préparation en cas d'incident



Commentaire du Commissariat à la protection de la vie privée du Canada relativement à l'intervention à la suite de la violation de données sur LinkedIn en 2012 :

« De toute évidence, la détermination de LinkedIn à résoudre le problème est venue du niveau le plus élevé, puisque les membres de la haute direction ont autorisé une intervention **« Code rouge »**, qui a accordé à l'incident une priorité absolue et déclenché le déploiement immédiat de ressources en vue de sa résolution. ... LinkedIn, comme de nombreuses autres organisations, aurait pu se doter de meilleures mesures de sécurité. Cela dit, en nous penchant sur l'intervention de l'organisation en réaction à la cyberattaque, nous avons constaté qu'elle avait fait preuve de la diligence et du sens des responsabilités requis. »

[Télécharger l'infographie](#)