Plan d'action pour un IC (en amont et non en aval)[1]

Afin de pouvoir réagir rapidement aux incidents de sécurité, susceptible d'impliquer des renseignements personnels, il est recommandé de considérer, entre autres, les éléments suivants :

Gouvernance, rôles et responsabilités au sein de la Centrale (amont)

- Posséder un organigramme institutionnel
- Liste des personnes clés formant l'équipe de gestion des incidents de sécurité : Responsable de la protection des renseignements personnels : Service TI et sécurité, juridique, communication, RH, Enquêteur interne / externe, Etc.
- Cartographie des renseignements personnels détenus (pour l'évaluation d'un incident de confidentialité) (voir autre document à remplir qui se nomme « cartographie des RP »)
- Inventaire des documents relatifs à la collecte, à l'utilisation, à la communication, à la conservation et à la sécurité des renseignements personnels : Politiques, procédures, lignes directrices, guides, formations offertes à l'interne, etc.
- Inventaire des mandats, contrats de service et ententes avec des tiers, des contrats d'assurance (assurance cybersécurité)
- Date des derniers tests d'intrusion, de simulation, des audits internes / externes et inventaire des mesures prises à la suite de ces tests / audits
- Plan financier – prévision d'un budget pour permettre la continuité des activités à la suite d'un incident de sécurité : Identifier, circonscrire, enquêter, corriger

Plan d'action : agir avec diligence et méthode (aval)

- Communiquer avec le responsable des TI et de la sécurité
- Communiquer avec le coordonnateur de l'équipe de gestion des incidents de sécurité, qui verra à impliquer les membres de cette dernière et toute

[1] Le présent document s'inspire grandement du texte suivant en y ajoutant et modifiant certains éléments pour refléter adéquatement la réalité des syndicats : https://cdn.ca.yapla.com/company/CPYY3Q7Y2h7Qix1QmIl4X3Rf/asset/files/Grille%20IC.pdf

autre personne susceptible d'aider à diminuer le risque, incluant le comité sur l'accès à l'information et la protection des renseignements personnels
- Aviser la haute direction et, selon la gravité de l'incident, le BP
- Conserver tous les documents en place au moment de l'incident sans les modifier, notamment pour préserver la preuve
- Modifier (révoquer) les accès et mots de passe
- Déterminer et documenter la cause et l'origine de l'incident (date, heure, lieu, support, cause interne ou externe, personne responsable)
- Déterminer et documenter les renseignements visés (personnels ou non), leur nombre et les personnes visées (employés, clients, etc.)
- Identifier, localiser et préserver les renseignements visés par l'incident
- Protéger la confidentialité des renseignements personnels visés et des autres
- Déterminer le risque de préjudice pour les personnes concernées (degré de sensibilité des renseignements en cause et probabilité que les renseignements aient été / soient sur le point d'être mal utilisé)
- Récupérer les renseignements personnels / les supports – obtenir une confirmation de destruction / de non-diffusion du responsable de l'incident
- Empêcher la diffusion / la divulgation des renseignements – chiffrement, blocage des accès
- Prendre les mesures correctives afin de circonscrire l'incident

Plan de communication interne

Aviser le personnel – insister sur le fait que l'incident n'a pas encore été révélé à l'externe – embargo jusqu'à telle date et les aviser de ne pas commenter publiquement

Plan de communication externe

Avis aux autorités (Commission d'accès à l'information, service de police, etc.)
Avis aux personnes concernées (et si décision de ne pas le faire, documenter les raisons ayant conduit à la décision de ne pas les aviser)
• Élaborer des modèles d'avis
Avis aux médias
• Communiqué de presse / Conférence de presse
• Déterminer qui interviendra
○ Rencontrer les répondants du centre d'appels

Sensibilisation sur l'incident
Scripts de réponse

Protéger / Prévenir / Suivi (sur une base régulière)

- Plan de continuité des activités
- Plan de surveillance
- Surveillance de crédit (Équifax, TransUnion, par ex.)
- Faire un suivi interne des mesures de sécurité, des politiques / procédures.
  adoptées / révisées à la suite de l'incident
- Possibilité de faire appel à un audit externe pour évaluer les mesures de sécurité; politiques / procédures adoptées / révisées à la suite de l'incident
- Plan « juridique »
  - Stratégie en cas de poursuite judiciaire
  - Enregistrer l'incident dans le registre des incidents
  - Couverture d'assurance
- Plan de communication interne et externe
  - Stratégie pour rétablir la confiance à l'interne, à l'externe (particuliers, partenaires)
  - Formation, sensibilisation

Schéma sur le traitement d'un IC