IIROC OCRCVM
Investment Industry Regulatory Organization of Canada
Organisme canadien de réglementation du commerce des valeurs mobilières

juno RISK SOLUTIONS

Gestion des cyberincidents
Guide de planification

À l'intention des courtiers membres de l'OCRCVM

Table des matières

1 Sommaire

Le présent guide est conçu pour aider les membres de l'OCRCVM à élaborer des plans efficaces d'intervention en cas de cyberincident. Conformément au *Guide des pratiques exemplaires en matière de cybersécurité* de 2015 de l'OCRCVM, il présente, à l'intention des courtiers membres de l'OCRCVM de petite et moyenne taille, un ensemble de stratégies, de lignes directrices et d'outils volontaires de cybersécurité pouvant servir à développer une capacité d'intervention face aux incidents de cybersécurité, et à réagir à ces derniers de manière efficace.

Ce guide n'est pas conçu pour servir de plan d'intervention fonctionnel. Chaque courtier membre doit plutôt établir des plans internes dans le cadre de sa stratégie de cybersécurité qui lui permettront de se préparer face aux risques auxquels il est le plus susceptible d'être confronté.

La **section 1** donne un bref aperçu de la cybersécurité et des principales normes en usage dans le secteur des valeurs mobilières.

La **section 2** présente une vue d'ensemble du cycle de vie d'un incident, des concepts de planification et d'importants outils sur lesquels faire reposer les plans d'intervention en cas d'incident.

La **section 3** traite de la question névralgique de la mobilisation externe. Cette mobilisation doit prévoir les rapports obligatoires dictés par le type de cyberincident en cause, de même que des rapports volontaires avec les principaux intervenants externes comme les organismes de réglementation, les clients, les partenaires, les fournisseurs externes et le gouvernement. Chacun de ces intervenants peut contribuer des éléments de soutien essentiels en réponse à un cyberincident.

L'**annexe A** renferme d'importantes recommandations pour instaurer une capacité d'intervention face incidents de cybersécurité et s'inspire du *Computer Security Incident Handling Guide* du National Institute of Standards and Technology (NIST). L'**annexe B** renferme un guide en dix étapes sur la façon de réagir à un incident de cybersécurité auquel votre organisation n'est pas préparée.

La planification de l'intervention en cas de cyberincident doit faire partie d'une stratégie exhaustive de cybersécurité. Cette planification doit être priorisée selon le type de risques auxquels l'entreprise est le plus susceptible d'être confrontée, aussi bien que de ceux qui pourraient avoir le plus de conséquences pour l'entreprise, pour ses relations et pour sa réputation. Le présent guide vous donnera les moyens d'amorcer ce travail de planification.

Le présent guide expose des pratiques courantes et des suggestions qui peuvent ne pas s'appliquer ou ne pas être pertinentes dans certains cas. Le document n'a pas pour objet de présenter une norme minimale ou maximale de ce qui constitue un plan d'intervention approprié en cas de cyberincident chez un courtier membre de l'OCRCVM. Un bon plan d'intervention

procède d'une analyse contextuelle de la situation qui est propre à chaque courtier.

Ce guide ne crée aucune nouvelle obligation légale ni ne modifie des obligations déjà imposées – comme les exigences actuelles de l'OCRCVM – et il ne vise nullement à le faire. L'information qu'il renferme est fournie uniquement à titre indicatif et nous ne pouvons pas garantir qu'elle est complète et exacte. Cette information ne doit pas être considérée non plus comme un avis juridique ou professionnel. Les courtiers membres qui désirent obtenir d'autres orientations devraient consulter un professionnel en cybersécurité pour obtenir des conseils précis sur leur programme de cybersécurité et leurs plans d'intervention en cas d'incident.

1.1 Toile de fond

Le paysage des cybermenaces dans le secteur financier évolue constamment; de nouvelles menaces émergent chaque jour.

Le renforcement des défenses à titre de pratique exemplaire adoptée par bon nombre d'institutions financières de plus grande taille a forcé les agents malveillants à s'adapter et à changer de cible pour s'attaquer aux vecteurs. C'est ainsi que les organisations de plus petite taille peuvent être ciblées – et l'ont d'ailleurs été – tant pour des gains financiers immédiats que pour un accès à l'infrastructure d'organisations plus grandes. Toute institution qui traite avec le public ou dont les activités font appel à l'Internet devrait se considérer comme exposée à une violation de ses données informatiques.

Il est donc essentiel que toutes les organisations – quelle que soit leur taille – renforcent leurs cyberdéfenses en fonction de la sensibilité de leurs actifs informationnels.

1.1.1 Objectifs

Le présent guide de gestion des cyberincidents est conçu pour aider les courtiers membres de l'OCRCVM de petite et moyenne taille à mieux se préparer à composer avec un cyberincident. Les entités de plus grande taille sont invitées à intégrer par renvoi leurs protocoles existants de gestion des incidents au présent guide, et à comprendre les processus que leurs pairs de taille plus modeste mettront en place en cas de crise.

Ce guide n'est pas conçu pour évaluer les cyberrisques qui pèsent sur une institution donnée. Les recommandations tiennent compte de l'apport d'un échantillon représentatif des membres de l'OCRCVM. Les courtiers membres qui souhaitent obtenir d'autres consignes peuvent charger un spécialiste de la cybersécurité de procéder à l'analyse complète de leur programme de cybersécurité et des plans connexes d'intervention en cas d'incident.

1.1.2 Contexte

Les incidents de cybersécurité ou les événements touchant les systèmes d'information des courtiers membres peuvent avoir d'importantes répercussions sur la prestation des services financiers. Il est essentiel de pouvoir réagir aux incidents de cybersécurité de façon cohérente et coordonnée, et en temps opportun.

Le présent guide s'inspire des principes de cybersécurité que l'on retrouve dans les publications suivantes :

Numéro de la norme	Titre
ISO/IEC 27035:2011	• Technologies de l'information – Techniques de sécurité – Gestion des incidents de sécurité de l'information
ISO/IEC 27035-1	• Principles of Incident Management (ébauche)
ISO/IEC 27035-2	• Guidelines To Plan And Prepare For Incident Response (ébauche)
ISO/IEC 27035-3	• Guidelines For Incident Response Operations
Publication spéciale 800-61 (révision 2) du NIST	• Computer Security Incident Handling Guide
Gouvernement du Canada	• Plan de gestion des incidents de la TI du gouvernement du Canada

2 Vue d'ensemble de la gestion des incidents de cybersécurité

La préparation aux incidents de cybersécurité et l'établissement d'un plan d'intervention peuvent être des processus ardus pour beaucoup d'organisations. Lorsque survient un tel incident, l'organisation doit prendre des mesures immédiates afin d'atténuer les menaces pour la confidentialité, l'intégrité et la disponibilité de ses actifs informationnels. Pour ce faire, il faut déployer efficacement des ressources et des stratégies de communication établies.

Les organisations ciblées doivent lutter farouchement contre les cybercriminels qui, s'ils disposent du temps et des fonds nécessaires, peuvent contourner les systèmes de défense les plus perfectionnés. Au nombre des principales sources de menaces, citons les initiés aux intentions malveillantes, les gens de confiance à l'interne dont les gestes occasionnent des dommages par erreur et les attaques de cybercriminels.

Les courtiers membres doivent prendre des mesures raisonnables pour gérer de façon appropriée un incident de cybersécurité. Une mauvaise exécution des mesures d'intervention en cas d'incident pourrait entraîner de lourdes pertes financières pour l'institution, ruiner sa réputation, et peut-être même l'obliger à mettre fin à ses activités[i].

Voici quelques-uns des principaux objectifs de la gestion des incidents de cybersécurité :

- Neutraliser les incidents de cybersécurité avant qu'ils ne surviennent
- Limiter l'impact des incidents de cybersécurité sur la confidentialité, la disponibilité ou l'intégrité des services, des actifs informationnels et des activités du secteur des valeurs mobilières
- Atténuer les menaces et les vulnérabilités des incidents de cybersécurité
- Améliorer la coordination et la gestion des incidents de cybersécurité au sein du secteur des valeurs mobilières

- Réduire les coûts directs et indirects engendrés par les incidents de cybersécurité
- Faire rapport des constatations à la haute direction

2.1 Termes et expressions clés

Les définitions qui suivent reposent sur la Norme internationale de gestion des incidents de sécurité de l'information (ISO/IEC 27035).[ii]

ÉVÉNEMENT DE CYBERSÉCURITÉ

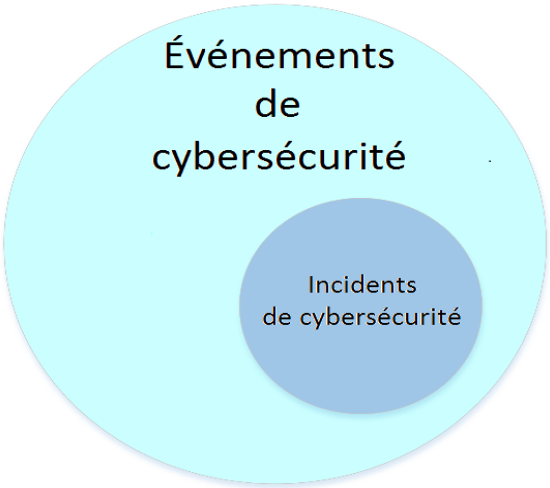
État d'un système, d'un service ou d'un réseau qui **indique une infraction possible** à la sécurité de l'information, une panne de contrôles ou une situation antérieure inconnue qui peut se rapporter à la sécurité.

INCIDENT DE CYBERSÉCURITÉ

Événement ou série d'événements non souhaités ou inattendus liés à la sécurité de l'information, qui sont **susceptibles de compromettre sensiblement les activités opérationnelles** et qui menacent la sécurité de l'information.

Les incidents de cybersécurité constituent une faible partie des événements.

Figure 1 – Événements de cybersécurité et incidents de cybersécurité[iii]



GESTION DES INCIDENTS DE CYBERSÉCURITÉ

Processus de détection, de signalement, d'évaluation, d'intervention, de traitement des incidents de cybersécurité, et qui permet d'en tirer des leçons.

INTERVENTION EN CAS D'INCIDENT

Mesures prises pour protéger et rétablir les conditions de fonctionnement normales d'un système d'information et des renseignements qui y sont stockés lors d'un incident de cybersécurité.

ÉQUIPE D'INTERVENTION EN CAS D'INCIDENT (EII)

Équipe de l'organisation dont les membres sont suffisamment compétents et dignes de confiance et qui prend en charge les incidents pendant leur cycle de vie.

2.2 Chaîne d'incident de cybersécurité

La Figure 1 présente les maillons de la chaîne d'incident de cybersécurité présentée dans la norme ISO 27035.

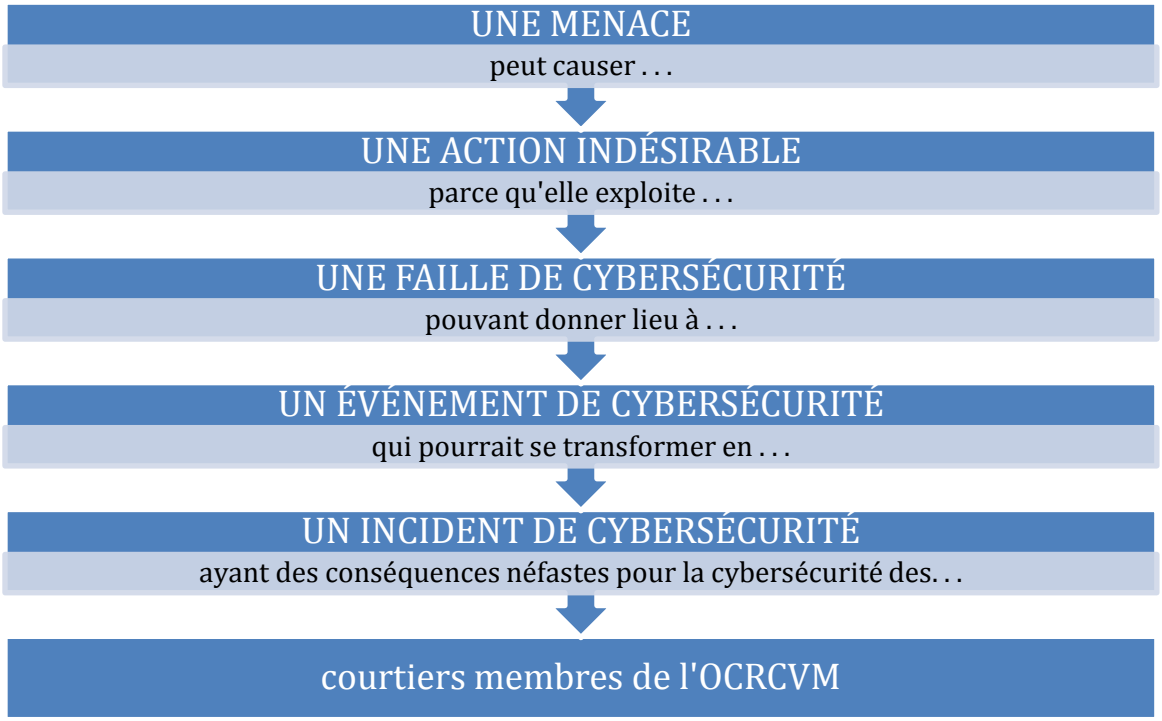


Figure 1 – La chaîne d'incident de cybersécurité

Schéma adapté à partir de la norme ISO/IEC 27035, *Technologies de l'information – Gestion des incidents de sécurité de l'information*

2.3 Intervenants

Intervenants primaires	Intervenants secondaires	Autres intervenants
• Clients • Autres courtiers membres (remisiers et courtiers chargés de comptes) • Fournisseurs de courtiers membres • OCRCVM	• Organisations spécialisées en sécurité (p. ex., le Centre canadien de réponse aux incidents cybernétiques (CCRIC)) • Commissariats à la protection de la vie privée • Organisations de partage volontaire de l'information	• Médias • Organismes fédéraux et régionaux d'application de la loi

2.4 Liste de contrôle d'un incident de cybersécurité

Le Tableau 1 ci-dessous énumère les processus et procédures qui doivent être en place avant, pendant et après un incident de cybersécurité[iv] :

LISTE DE CONTRÔLE D'UN INCIDENT DE CYBERSÉCURITÉ

AVANT UN INCIDENT

- Dresser une liste priorisée des actifs informationnels d'une importance critique pour le bon fonctionnement de votre organisation.
- Identifier les intervenants responsables de chaque actif d'une importance critique.
- Mettre sur pied une équipe d'intervention en cas d'incident qui sera chargée de tous les incidents (comprenant des représentants des services juridiques, des communications et des ressources humaines).
- Veiller à ce que des technologies pertinentes de surveillance et de suivi soient en place pour protéger les actifs informationnels de votre organisation (notamment des pare-feu, des systèmes de prévention des intrusions (SPI) et des antivirus).
- Fournir une formation média aux personnes compétentes.
- Mettre en place un processus à la grandeur de l'organisation pour permettre aux employés, aux sous-traitants et aux tiers de signaler les activités suspectes ou les soupçons de piratage.
- Donner de la formation dans toute l'organisation au sujet de la sensibilisation aux infractions, de la responsabilité des employés et des processus de signalement.

PENDANT UN INCIDENT

- Consigner les problèmes et préparer un rapport d'incident.
- Convoquer l'équipe d'intervention en cas d'incident (EII).
- Organiser une téléconférence avec les intervenants compétents pour discuter des mesures à prendre pour rétablir les activités.
- Organiser une téléconférence avec les intervenants compétents pour faire le point sur la situation avec la haute direction.
- Trier les enjeux actuels et les communiquer à la haute direction.
- Déterminer la cause initiale de l'incident et convoquer les spécialistes pour corriger les problèmes afin de rétablir les activités.
- Conserver les éléments de preuve et suivre une chaîne de preuves rigoureuse à l'appui de toute mesure juridique nécessaire ou prévue.
- Communiquer avec les tiers visés, les organismes de réglementation et les médias (si nécessaire).

APRÈS UN INCIDENT

- Mettre à jour le rapport d'incident et déterminer exactement ce qui est arrivé et à quel moment.
- Vérifier dans quelle mesure le personnel et la direction ont bien agi au cours de l'incident.
- Déterminer si les procédures documentées ont été suivies.
- Discuter des changements qu'il faudra apporter aux processus ou à la technologie pour atténuer les incidents futurs.
- Déterminer les renseignements qui auraient dû être fournis plus tôt.
- Déterminer si les étapes appliquées ou les mesures prises auraient pu nuire à la reprise.
- Préciser les outils ou autres ressources nécessaires pour détecter, trier, analyser et

atténuer les incidents futurs.

- Discuter des exigences de signalement nécessaires (notamment au chapitre de la réglementation et de la clientèle).

- Dans la mesure du possible, quantifier les pertes financières causées par l'infraction.

Tableau 1 – Liste de contrôle pour la gestion des incidents de cybersécurité

2.5 Les cinq phases de la gestion d'un incident de cybersécurité

La Figure 3 présente les cinq phases de la gestion d'un incident de cybersécurité.

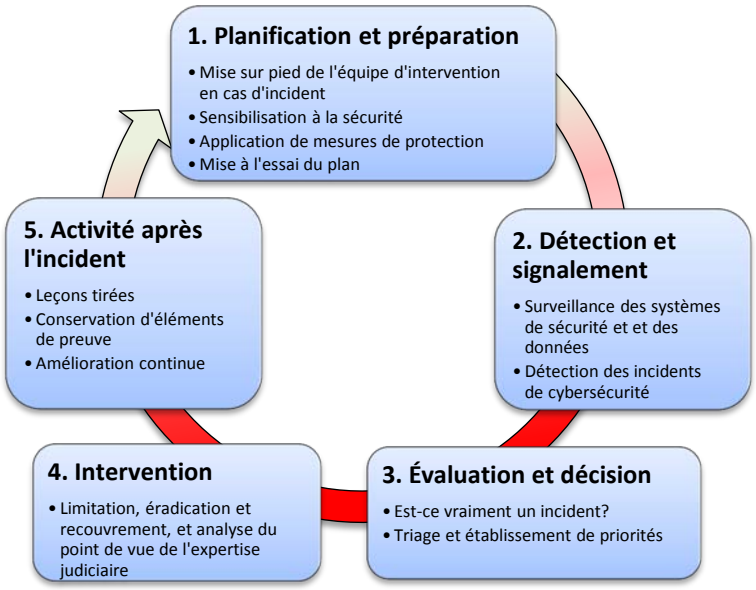
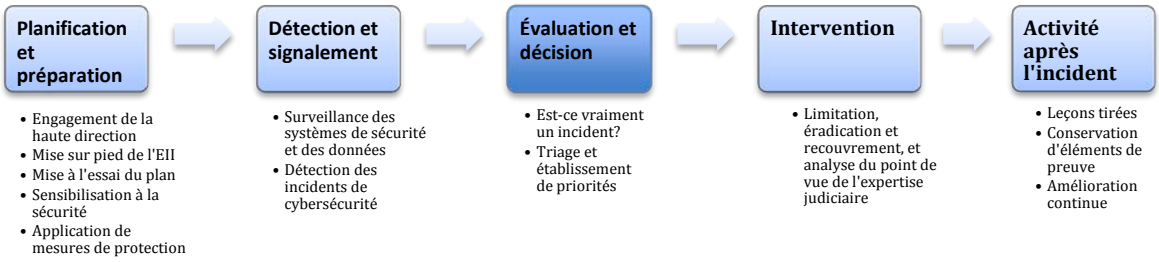


Figure 3 – ***5 éléments clés de la gestion d'un incident de cybersécurité***

2.5.1 Planification et préparation



Planifier et préparer un plan de gestion d'incident de cybersécurité pour que votre organisation soit prête à intervenir lorsque survient un incident de cybersécurité.

Pour se préparer à un incident de cybersécurité, les intervenants doivent songer à exécuter les **activités clés** suivantes :

- Obtenir l'appui de la haute direction à l'égard du plan de gestion des incidents de cybersécurité.
- Établir une capacité formelle d'intervention en cas d'incident de cybersécurité afin de réagir promptement et efficacement lorsque la sécurité informatique est compromise[v].
- Établir une politique de gestion des incidents de cybersécurité qui décrit les types d'événements qui doivent être considérés comme des incidents; cette politique établit la structure organisationnelle d'intervention en cas d'incident; définit les rôles et les responsabilités; et énonce les exigences redditionnelles[vi].
- Élaborer des procédures d'intervention en cas d'incident. Ces procédures expliquent en détail comment intervenir à la suite d'un incident. Elles doivent traiter de toutes les étapes du processus d'intervention et s'appuyer sur la politique et sur le plan de gestion des incidents de cybersécurité[vii].
- Établir des politiques et des lignes directrices sur la coopération interne et externe ainsi que le partage de l'information.
- Prendre connaissance des actifs informationnels qu'il vous incombe de protéger. Vos données doivent être répertoriées en fonction de leur criticalité et de leur sensibilité opérationnelles. Les détails recueillis doivent notamment indiquer qui est propriétaire de l'actif informationnel, où ce dernier est stocké et quels contrôles sont en place en vue de le protéger. Les contrôles eux-mêmes doivent faire l'objet d'un suivi. *Il importe avant tout de comprendre ce que serait l'impact potentiel de la perte de l'actif informationnel.*
- Mettre en œuvre des contrôles afin de protéger les actifs informationnels de votre organisation. À titre d'exemple de ces contrôles, citons les pare-feu, la gestion des correctifs et l'évaluation de la vulnérabilité.
- Réunir une EII.
- Assurer la formation des membres de l'EII.

- Élaborer un plan de communication et une formation en matière de sensibilisation pour tout le personnel de l'organisation.
- Fournir des mécanismes simples aux fins de la reddition de comptes.
- Déployer des contrôles de sécurité des terminaux (des scanners anti-maliciels, p. ex.) sur les systèmes d'information. Veiller à ce que les bases de données de ces scanners et autres contrôles de point terminal soient fréquemment mises à jour. L'abonnement à des services de sécurité comme les logiciels anti-maliciels doit habituellement être renouvelé chaque année. Si l'abonnement vient à échéance, vos systèmes d'information seront aussitôt exposés aux cybermenaces.
- Établir des liens avec les organismes d'application de la loi et des équipes externes d'intervention en cas d'incident.
- Évaluer la capacité de réponse à un incident, notamment grâce à des simulations.

Le schéma d'événement et d'incident de cybersécurité ci-après donne une vue d'ensemble de la gestion des incidents de cybersécurité.

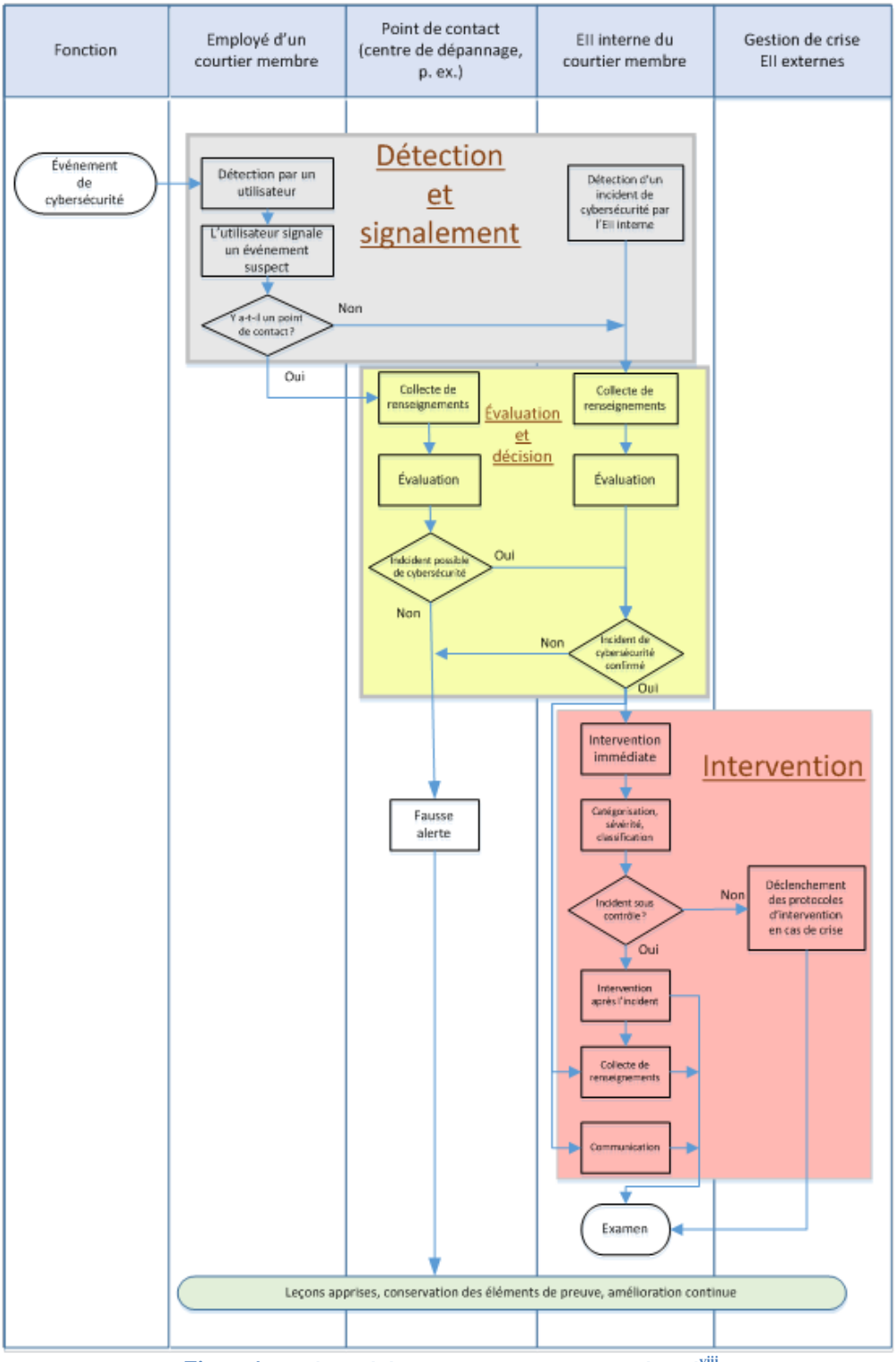
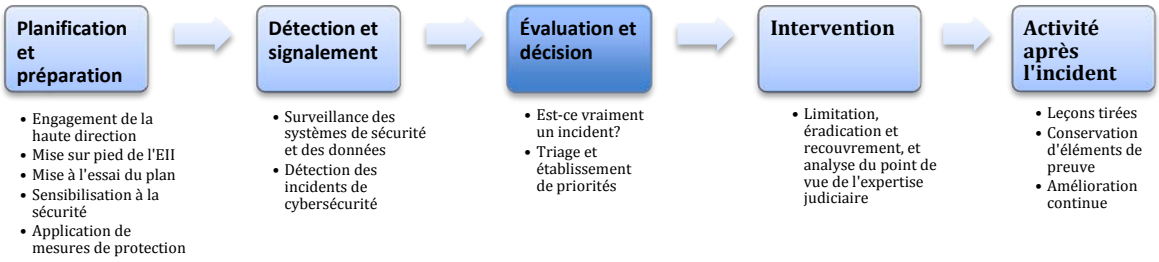


Figure 4 – Schéma d'événement et d'incident de cybersécurité[viii]

2.5.2 Détection et signalement



Cette phase repose sur le suivi continu des sources de renseignements, sur la détection d'un événement de cybersécurité, de même que sur la collecte et la consignation de renseignements liés à l'événement.

Activités clés :

- Surveiller les rapports d'activité inusitée soumis par les utilisateurs.
- Surveiller les alertes transmises par les systèmes de sécurité internes.
- Surveiller l'information communiquée par les organisations pairs, les fournisseurs et les organisations spécialistes des incidents de cybersécurité comme le Centre canadien de réponse aux incidents cybernétiques (CCRIC) et le Financial Services Information Sharing and Analysis Center (FS-ISAC).
- Surveiller les alertes diffusées par les sources de renseignements externes comme les équipes nationales d'intervention en cas d'incident, les organismes d'application de la loi, etc.
- Surveiller les indices d'activités inusitées dans les systèmes ou le réseau.
- Recueillir l'information pertinente.
- Poursuivre la surveillance et la détection.
- Acheminer les rapports d'activité inusitée à l'EII.

2.5.2.1 Causes possibles d'un incident de cybersécurité

Voici des causes possibles d'incidents de cybersécurité :

- Tentative d'accès non autorisé à un système ou à ses données
- Tentative visant à perturber la prestation des services d'une organisation
- Accès non autorisé à des systèmes d'information
- Modification non autorisée de systèmes d'information
- Infection au moyen d'un maliciel
- Initié de confiance aux intentions malveillantes
- Courriel renfermant un maliciel
- Utilisation d'un support amovible infecté (une clé USB, p. ex.)

- Utilisateur utilisant un moteur de recherche pour consulter un site Internet qui exploite une faille du moteur de recherche en question
- Vol ou perte d'un système d'information comme un ordinateur portable ou un téléphone intelligent

2.5.2.2 Signes de possible compromission d'un système d'information

Voici des signes d'une possible compromission d'un système d'information :

- Les comptes ou les mots de passe ne fonctionnent plus
- Le site Internet de l'entreprise renferme des modifications non autorisées
- Il n'y a plus d'espace disque ou de mémoire disponible
- Le système ne peut plus se connecter au réseau
- Le système gèle à répétition ou se réinitialise de façon imprévue
- Le moteur de recherche sur Internet ne fonctionne plus comme prévu
- Les contacts d'un carnet d'adresses reçoivent des pourriels de l'adresse du propriétaire de ce carnet d'adresses
- Les contrôles de sécurité des terminaux, comme les antivirus, ne fonctionnent plus
- Les contrôles de sécurité des terminaux, comme les antivirus, signalent que le système d'information lui-même a été la cible d'une tentative de compromission
- Les registres du système d'information font état d'activités suspectes

2.5.2.3 Ce qu'il faut signaler et ne pas signaler à l'EII

Il importe que tous les utilisateurs sachent quand ils doivent signaler une activité suspecte à leur EII, et quand il n'y a pas lieu de le faire. Il faut donner aux utilisateurs la consigne de communiquer avec le service de dépannage ou directement avec l'EII s'ils croient qu'un incident a pu survenir.

Le Tableau 2 ci-après donne des exemples de situations où il convient de signaler un incident suspect à l'EII.

Voici des exemples d'événements qui **doivent être signalés** à l'EII :

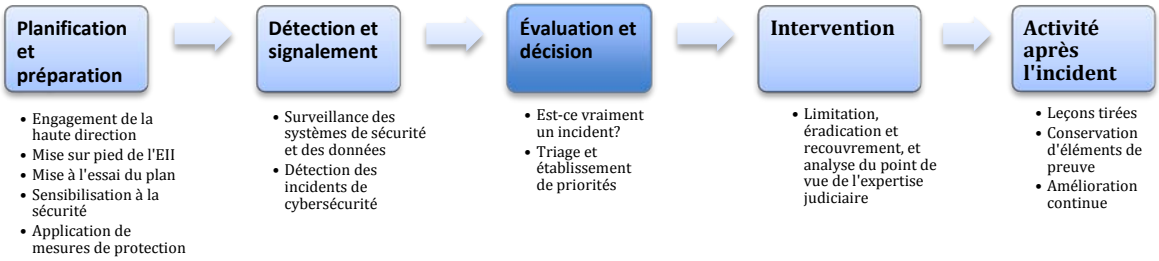
- Courriels suspects renfermant des pièces jointes ou des hyperliens
- Atteinte à la protection des données
- Perte ou vol des appareils électroniques de votre organisation (p. ex., ordinateurs portables et téléphones intelligents)
- Systèmes d'information critiques infectés par des virus ou d'autres maliciels
- Attaques en déni de service
- Activités suspectes ou non autorisées sur le réseau
- Défaillance des systèmes, des services ou des réseaux du courtier membre
- Piratage ou compromission de la présence en ligne de votre organisation

Suivent des exemples d'événements qu'**il n'y a pas lieu de signaler** à l'EII, mais dont il faudrait aviser le service de dépannage.

- Activités ponctuelles de virus faciles à neutraliser et qui n'ont pas d'impact sur les systèmes critiques de l'organisation
- Brèves pannes de services non critiques
- Cas ponctuels de pourriels classiques dépourvus de liens ou de pièces jointes malveillants
- Manquement, de la part d'un utilisateur, à certaines politiques ou lignes directrices organisationnelles relatives à Internet

Tableau 2 – Ce qu'il faut signaler à l'EII

2.5.3 Évaluation et décision



Cette phase consiste à évaluer les *événements* de cybersécurité et à déterminer si un incident de cybersécurité est bel et bien survenu.

L'évaluation débute lorsque des signes indiquent qu'un événement de cybersécurité s'est produit. Les membres de l'EII et le personnel du centre de dépannage peuvent effectuer une première évaluation en utilisant des critères préétablis semblables à ceux énoncés au Tableau 2 pour déterminer si l'événement constitue vraiment un incident. Si l'organisation conclut à un incident de cybersécurité, elle doit en déterminer l'impact sur la confidentialité, l'intégrité et la disponibilité de l'actif informationnel touché.

Les incidents de cybersécurité représentent une faible proportion des événements de cybersécurité.

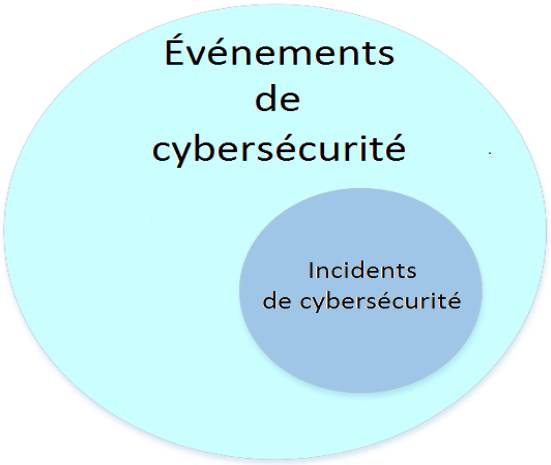
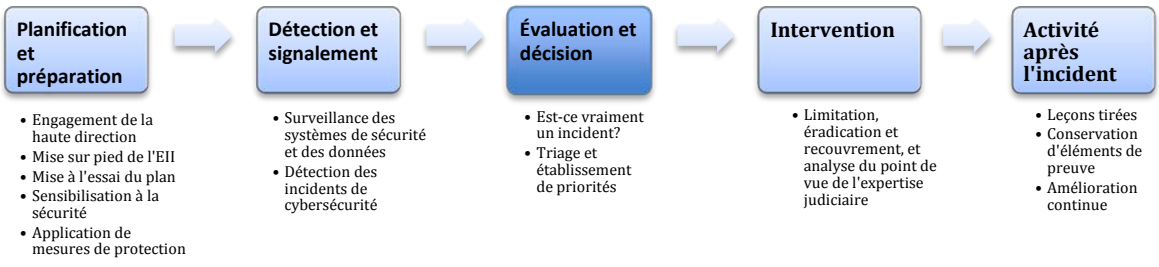


Figure 2 – Lien entre les incidents et les événements de cybersécurité[ix]

Tâches :

- Désigner la personne qui sera responsable de l'événement.
- Déterminer si l'événement est un véritable incident de cybersécurité ou une fausse alerte.
- Si un incident de cybersécurité est survenu, il doit être signalé à l'EII.
- Déterminer quels renseignements, systèmes ou réseaux sont touchés.
- Cerner l'impact sur la confidentialité, l'intégrité et la disponibilité.
- Aviser les personnes compétentes.
- Vérifier si vos partenaires en affaires sont touchés.

2.5.4 Intervention



Intervenir en réponse à un incident (p. ex., le contenir, le soumettre à une enquête et le régler).

Tâches :

- Mobiliser des ressources internes et recenser des ressources externes afin d'intervenir en réponse à l'incident.
- Confiner le problème en mettant le système hors circuit ou en le déconnectant du réseau, par exemple.
- Éliminer les composantes malveillantes de l'incident en supprimant les maliciels ou en fermant un compte d'utilisateur piraté, par exemple.
- Se remettre de l'incident en rétablissant les activités normales des systèmes et en corrigeant les vulnérabilités pour éviter d'autres incidents similaires.
- Procéder au besoin à l'analyse judiciaire de l'incident.

➔ Les procédures de communication, de signalement et d'acheminement aux échelons supérieurs à appliquer lors d'une intervention face à une crise sont décrites à l'annexe A.

2.5.4.1 Quatre catégories d'intervention en cas d'incident de cybersécurité

L'étape d'intervention vise à atténuer l'impact des menaces et des vulnérabilités sur le système d'information touché et d'en rétablir le fonctionnement normal. On dénombre quatre catégories d'intervention nécessaires face à un incident de cybersécurité[x] :

INTERVENTION TECHNIQUE

L'intervention technique cible les mesures prises par le personnel technique afin d'analyser et de dénouer un événement ou un incident. Le personnel technique comprend les groupes de TI dont les services sont requis pour aider à mettre fin à l'événement ou à l'incident. Cela peut faire appel à plusieurs groupes ou services de TI afin de coordonner et de prendre les mesures techniques nécessaires pour confiner, dénouer ou atténuer les incidents, et pour réparer et remettre en état, au besoin, les systèmes ou les données touchés.

INTERVENTION DE LA DIRECTION

L'intervention de la direction met en lumière les activités nécessitant la contribution ou l'interaction de la direction, le signalement de l'événement ou de l'incident à la direction ou l'approbation de cette dernière. Elle peut englober la coordination des communications intégrées relativement à toute question de ressources humaines, de relations publiques, de comptabilité financière, d'audit ou de conformité.

INTERVENTION DE COMMUNICATION

Ces activités font appel à la communication avec la société et avec ses composantes internes et externes. Le service des communications de la société doit toujours être consulté avant la diffusion de tout message. Dans bien des cas, la direction dirigera la diffusion de renseignements relatifs à l'infraction.

INTERVENTION JURIDIQUE

Si elle est nécessaire, l'intervention juridique fera appel à des organismes de réglementation de l'extérieur, à des tiers et à d'autres intervenants. Il faudrait aussi obtenir des avis juridiques relativement à toute communication externe pour assurer le respect de la politique de l'entreprise et de toute exigence législative ou réglementaire.

2.5.4.2 Quatre niveaux d'intervention face à un incident de cybersécurité pour les courtiers membres de petite et moyenne taille

La section précédente décrivait les différentes mesures d'intervention qu'un courtier membre peut prendre. La présente section aborde les différents stades ou *niveaux d'intervention*. Les stades d'intervention vont des activités courantes normales, qui se déroulent en l'absence d'un incident de cybersécurité, à la survenance d'un cyberincident carabiné qui touche de nombreux courtiers membres. Ces niveaux d'intervention dictent l'ampleur de la coordination requise en réponse à un incident de cybersécurité donné. Au nombre des éléments, citons des déclencheurs et des niveaux de signalement aux échelons supérieurs, la participation des intervenants et la présentation de rapports.

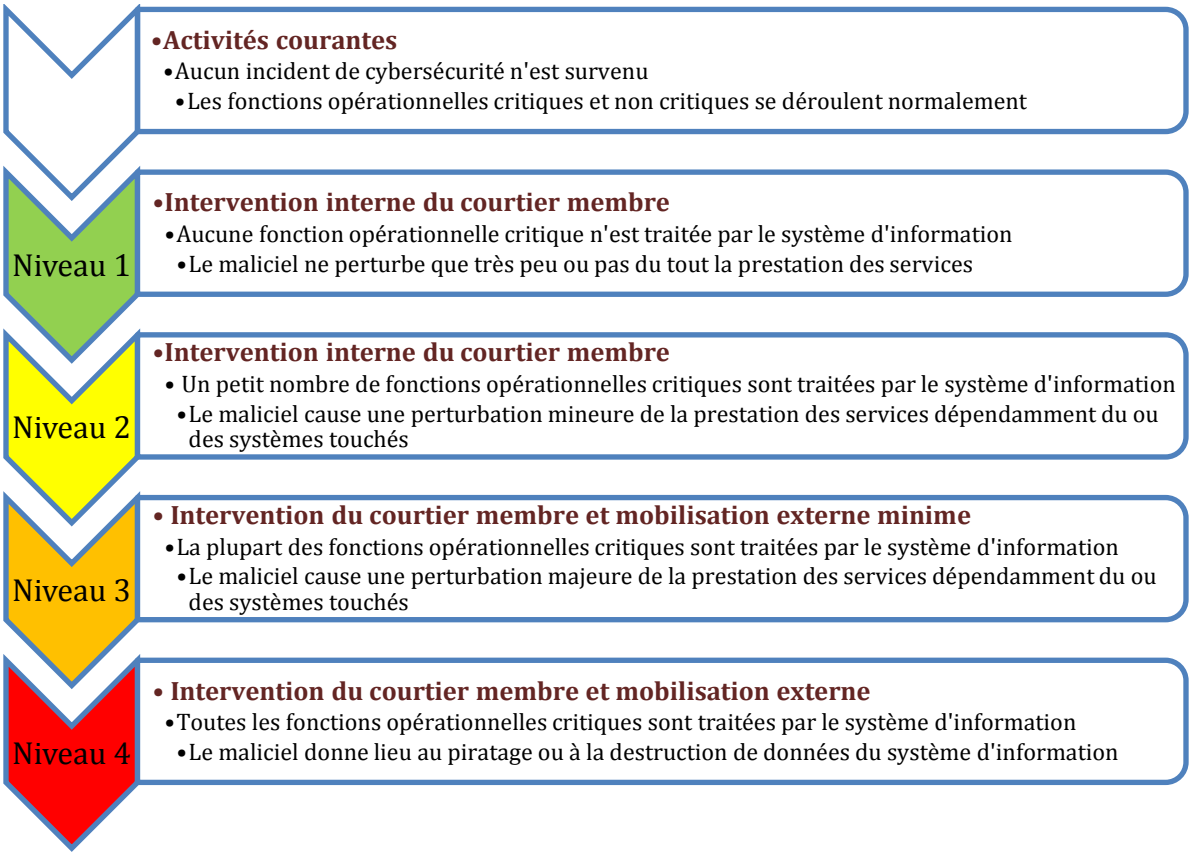


Figure 3 – Niveaux d'intervention pour les courtiers membres de l'OCRCVM de petite et moyenne taille

Niveau d'intervention 1 – Perturbation très légère ou nulle de la prestation des services

Ce niveau correspond aux activités courantes normales. Il peut y avoir des tentatives d'infection d'un système d'information non critique, mais les contrôles de point terminal comme

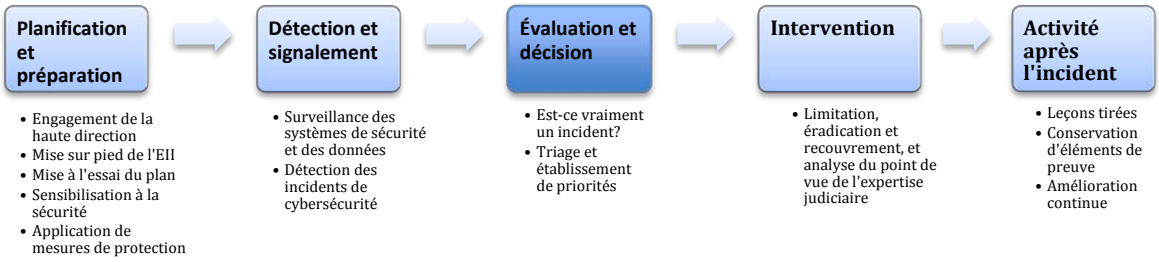
les antivirus y font obstacle et suppriment la menace. Si un système non critique est infecté, le service de dépannage de l'organisation peut éliminer la menace et rétablir le fonctionnement normal du système. Il n'y a pas lieu de signaler des situations à l'EII du courtier.

Niveau d'intervention 2 – Perturbation mineure de la prestation des services
Ce niveau correspond à un stade d'alerte plus élevé pour le courtier membre. Un maliciel peut avoir infecté de nombreux systèmes d'information non critiques et quelques systèmes d'information critiques. Il faudra porter la situation à l'attention de l'EII pour aider à évaluer la situation et à atténuer l'impact de l'exposition. Si l'EII et les intervenants pertinents estiment qu'il n'y a pas eu d'impact sur les fonctions opérationnelles critiques de l'organisation, ils pourraient réagir en procédant à une mise à jour urgente du scanneur de maliciels ou en déclenchant le processus de gestion des correctifs urgents.

Niveau d'intervention 3 – Perturbation majeure de la prestation des services
Ce niveau indique que l'EII du courtier membre doit intervenir sans délai. Un maliciel pourrait avoir compromis les systèmes d'information critiques du courtier membre. Le passage à ce niveau déclenchera une intervention centralisée et coordonnée des intervenants au sein du courtier membre. Les intervenants externes comme les fournisseurs spécialisés en intervention en cas d'incident, les organismes d'application de la loi et le CCRIC pourraient être mobilisés. Les interventions peuvent obliger tous les courtiers membres à installer des mises à jour urgentes ou contraindre le courtier touché à débrancher ses systèmes de l'Internet.

Niveau d'intervention 4 – Incident de cybersécurité catastrophique
Ce niveau ne s'applique qu'aux incidents de cybersécurité graves ou catastrophiques. L'infrastructure du courtier membre a pu être détruite, tout comme les données de ses systèmes d'information d'importance critique. Les incidents de cette gravité nécessiteront la mobilisation des intervenants externes comme l'OCRCVM, le CCRIC, les organismes d'application de la loi, les fournisseurs spécialisés, les organismes de réglementation pairs et tous les organismes gouvernementaux pertinents.

2.5.5 Activité après l'incident



La **phase consécutive à l'incident** permet notamment de tirer des leçons de l'incident et d'apporter des changements qui amélioreront la sécurité et les processus.

Tâches :

- Dégager les leçons tirées de l'incident de cybersécurité.
- Cerner des améliorations à apporter à l'architecture de sécurité de l'organisation, et les apporter.
- Déterminer l'efficacité avec laquelle le plan d'intervention en cas d'incident a été exécuté lors de l'incident de cybersécurité.

Il s'agit de l'un des plus importants volets de l'intervention en cas d'incident de cybersécurité. Il est très utile pour améliorer les mesures de sécurité et le processus de gestion des incidents de cybersécurité lui-même. Il permet de tourner la page à la suite d'un incident en passant en revue ce qui s'est produit, les mesures d'intervention qui ont été prises et l'efficacité de cette intervention.

3 Partage de l'information

3.1 Partager l'information avec des intervenants de l'extérieur

Il a été démontré que le partage de l'information avec les intervenants de l'extérieur est l'une des stratégies de cyberdéfense les plus efficaces. Cette affirmation est fondée sur le principe selon lequel un incident de sécurité qui touche une institution est un avertissement pour les autres institutions. Le partage des renseignements sur les cybermenaces peut accélérer sensiblement les préparatifs des interventions.

Avant de demander une aide extérieure ou de signaler la situation à des intervenants de l'extérieur, les sociétés doivent absolument comprendre tant l'obligation de signalement que celle de protéger l'information de nature délicate.

Voici les principaux facteurs à considérer pour planifier le partage de l'information :

- Pourquoi – Comprendre l'objet de l'échange envisagé
- Quoi – Déterminer précisément quels renseignements seront partagés, et leur niveau de détail
- Qui – Choisir les intervenants avec lesquels l'information sera partagée
- Quand – Décider du moment où les renseignements seront partagés
- Comment – Choisir la méthode d'échange et les mesures de protection à appliquer

Principaux acteurs dans la planification de l'information sur la cybersécurité[xi]

Les catégories de partenaires suivantes aideront à planifier une stratégie de mobilisation et peuvent être considérées comme des maillons de la chaîne d'information en cas de cyberincident :

Gouvernement – Au Canada, le Centre canadien de réponse aux incidents cybernétiques (CCRIC) est le principal intermédiaire entre le gouvernement et le secteur privé lorsqu'il faut intervenir en réponse à un incident. Le CCRIC fournit une gamme de produits de signalement aux sociétés canadiennes. Chaque signalement d'un cyberincident au CCRIC peut être une excellente occasion de recueillir des renseignements.

Infrastructure critique privée – D'autres participants du secteur des services financiers canadiens peuvent appuyer les interventions en réponse aux incidents en fournissant des renseignements liés à leur expérience de problèmes similaires. À moins que l'incident ne soit jamais survenu auparavant, une mobilisation externe efficace permettra de recueillir des renseignements.

Entreprises commerciales – D'autres sociétés de l'extérieur du secteur des services financiers ont peut-être acquis une précieuse expérience de menaces similaires. Chaque entreprise a intérêt à protéger ses réseaux et ses renseignements d'une importance critique.

Sociétés de TI – Les entreprises qui créent des produits de TI ont intérêt à protéger leurs produits et leurs clients. Elles échangent souvent des renseignements sur les vulnérabilités de leurs produits et services pour que les entreprises de sécurité puissent mettre au point des défenses plus efficaces. La mobilisation des fournisseurs de certains produits peut accélérer les cycles de vie des produits.

Sociétés de sécurité de la TI – Ces entreprises peuvent constituer à la fois un rouage essentiel de l'intervention face à un incident et une source de renseignements en vue de réagir aux menaces.

Chercheurs en sécurité – Ces chercheurs travaillent dans le milieu universitaire, des affaires ou dans d'autres secteurs de collaboration volontaire qui appuient la cybersécurité collective. Ils sont à la fois une source de renseignements et d'éventuels partenaires lors d'une intervention en réponse à un incident. La compréhension de la composition de cette ressource peut être une activité utile de préparation à un incident.

3.2 Ententes de partage et exigences de signalement des infractions

Le partage de l'information devrait procéder à la fois de préoccupations au sujet du partage permissif volontaire visant à réaliser les objectifs institutionnels et du signalement obligatoire des cas de piratage reposant sur les obligations imposées par la loi. Ces obligations sont propres à chaque entreprise et dépendent des marchés sur lesquels l'entreprise évolue ainsi que de la nature des renseignements piratés.

Lorsque l'on envisage le partage permissif de renseignements avec des intervenants de l'extérieur, les mesures de protection déjà instaurées en prévision d'un incident, comme les accords réciproques de confidentialité et les modalités contractuelles semblables, peuvent aider à établir clairement les règles de base régissant l'échange.

3.2.1 Signalement des atteintes ayant trait aux renseignements personnels

En juin 2015, la *Loi sur la protection des renseignements personnels numériques* (LPRPN) a modifié la loi fondamentale du Canada qu'est la *Loi sur la protection des renseignements personnels et des documents électroniques* (LPRPDE) afin de stipuler qu'une organisation sera tenue de signaler au commissaire à la protection de la vie privée « toute atteinte aux mesures de sécurité qui a trait à des renseignements personnels dont elle a la gestion, s'il est raisonnable de croire, dans les circonstances, que l'atteinte présente un risque réel de préjudice grave à l'endroit d'un individu ». La LPRPN prévoit des amendes pouvant atteindre 100 000 $ en cas de dérogation volontaire à l'obligation pour les organisations de signaler les atteintes et de tenir et de conserver un registre de toutes les atteintes aux mesures de sécurité qui ont trait à des renseignements personnels dont elles ont la gestion.

Les exigences de signalement des atteintes ne seront pas appliquées tant que les mesures réglementaires connexes n'auront pas été promulguées. De toute évidence, les exigences canadiennes en matière de signalement des atteintes sont en train de changer et les sociétés doivent se tenir bien au fait de ces dispositions.

La LPRPDE ne s'applique pas dans les provinces où le gouvernement fédéral est d'avis qu'il existe une loi sur la protection des renseignements personnels essentiellement similaire à la LPRPDE. À l'heure actuelle, l'Alberta, la Colombie-Britannique et le Québec sont les seules provinces dont la législation sur la protection des renseignements personnels a été déclarée

essentiellement similaire à la LPRPDE, et seule la loi albertaine comporte des dispositions sur le signalement obligatoire des atteintes. Les entreprises doivent prendre connaissance des dispositions sur le signalement des atteintes qu'applique chacun des territoires où elles exercent leurs activités, et adopter des politiques internes conformes à la législation pertinente.

3.2.2 Partage de l'information

Les cybermenaces sont de nature planétaire; elles ne se limitent pas à une entreprise, à un secteur ou à un marché en particulier. Le partage de l'information est une composante essentielle d'un programme efficace de cybersécurité. Les participants au marché du secteur financier considèrent de plus en plus la cybersécurité comme un bien collectif. Les doutes à propos de l'intégrité d'un participant au marché peuvent rapidement se propager à d'autres. Les membres du secteur des services financiers sont disposés à partager les pratiques exemplaires de cybersécurité et les renseignements qui se rapportent aux menaces.

La LPRPN utilise aussi un langage plus permissif que les lois précédentes, lequel permet aux organisations de partager de l'information entre elles pour déceler ou contrer un acte de fraude susceptible d'être perpétré, ou en vue d'une enquête sur la violation d'un accord ou sur la contravention au droit fédéral ou provincial qui a été commise ou qu'il est raisonnable de croire qu'elle pourrait l'être. Alors que la législation antérieure exigeait qu'il existe un organisme d'enquête reconnu, celle en vigueur semble permettre aux secteurs d'échanger plus efficacement des renseignements pertinents en matière de cybersécurité et d'autres renseignements relatifs à la sécurité afin de protéger leurs intérêts. Le secteur canadien des valeurs mobilières est bien placé pour emboîter le pas à ceux des banques et des sociétés d'assurance-vie pour mettre en place tant des accords spéciaux que des accords structurés de partage de l'information à l'appui des programmes de cybersécurité des sociétés.

Le partage des renseignements est un outil essentiel pour atténuer les cybermenaces. Cet outil est à la fois stratégique, tactique, opérationnel et technique, et il couvre toutes les étapes du cycle d'intervention en réponse à un cyberincident. Il transcende la frontière entre les domaines public et privé. Enfin, il peut englober des renseignements de nature délicate qui pourraient être préjudiciables à une organisation donnée tout en étant très utiles pour d'autres[xii].

3.3 Techniques de partage des renseignements

Les renseignements peuvent être partagés de diverses façons selon l'étendue et la profondeur de la relation en la matière et des intentions des parties. En prévision d'un cyberincident, les entreprises devraient se pencher sur les parties avec lesquelles elles seraient susceptibles d'échanger des renseignements, et sur la nature de leur approche. Voici des exemples de techniques de partage de renseignements :

- de façon ponctuelle, de personne à personne;
- de machine à machine à l'aide de protocoles structurés de renseignements sur les menaces;

- par échange structuré formel selon des protocoles et des seuils de divulgation convenus.

Les tribunes d'échange existantes comme celles qu'animent le FS-ISAC ou le CCRIC facilitent l'échange anonyme de données sur les incidents et les menaces entre les participants. L'échange moins formel entre des groupes de sociétés ou entre des membres de l'OCRCVM devrait être défini en prévision d'un incident afin que la société visée tire une valeur de l'échange et sache que l'information partagée sera protégée.

4 Annexes

Annexe A : Principales recommandations pour la mise en place d'une capacité d'intervention en cas de cyberincident

Le *Computer Security Incident Handling Guide* du NIST énonce les recommandations clés suivantes pour mettre en place une capacité d'intervention en réponse à un incident de cybersécurité :

- **Acquérir des outils pouvant être utiles pour traiter les incidents.** L'équipe de l'entreprise traitera les incidents de façon plus efficiente si elle dispose déjà de divers outils et ressources comme des listes de personnes-ressources, des logiciels de cryptage, des schémas de réseaux, des dispositifs de sauvegarde, des logiciels d'analyse et des listes de ports.
- **Prévenir les incidents en veillant à ce que les réseaux, les systèmes et les applications soient adéquatement sécurisés.** L'évaluation périodique des risques et la prise de mesures pour ramener les risques connus à des niveaux acceptables sont des façons efficaces de réduire le nombre d'incidents. Il est aussi très important que les utilisateurs, les préposés à la TI et les dirigeants soient au fait des politiques et des procédures de sécurité.
- **Déceler les signes précurseurs et les indicateurs grâce aux alertes générées par les logiciels de sécurité.** Les systèmes de détection et de prévention des intrusions, les antivirus et les logiciels de contrôle de l'intégrité des fichiers sont utiles pour déceler les signes d'incidents. Comme chaque type de logiciel peut déceler des incidents que d'autres logiciels ne relèvent pas, on recommande vivement d'utiliser plusieurs types de logiciels de sécurité informatique. Les services de contrôle offerts par des tiers peuvent également être utiles.
- **Mettre en place des mécanismes permettant aux intervenants de l'extérieur de signaler des incidents.** Les intervenants de l'extérieur pourraient vouloir signaler des incidents à l'organisation croyant, par exemple, qu'ils sont la cible d'une attaque de la part de l'un des utilisateurs de l'organisation. Les organisations devraient communiquer un numéro de téléphone et une adresse de courriel que les intervenants de l'extérieur peuvent utiliser pour signaler de tels incidents.
- **Établir des normes minimales de tenue de registres et d'audit visant tous les systèmes, et des normes plus élevées en la matière visant tous les systèmes critiques.** Les registres des systèmes opérationnels, des services et des applications sont souvent utiles pour l'analyse des incidents, surtout si des audits ont été réalisés. Ces registres peuvent notamment indiquer quel compte a été utilisé et quelles opérations ont été effectuées.
- **Profiler les réseaux et les systèmes.** Le profilage mesure les caractéristiques de niveaux prévus d'activité pour que les changements des tendances soient plus faciles à déceler.

Si le profilage est automatisé, les déviations par rapport aux niveaux prévus d'activité peuvent être décelés et signalés rapidement aux administrateurs, ce qui accélère la détection des incidents et des problèmes opérationnels.

- **Comprendre le comportement normal des réseaux, des systèmes et des applications.** Les membres de l'équipe qui comprennent le comportement normal devraient pouvoir relever plus facilement les comportements anormaux. La meilleure façon de procéder consiste à examiner les entrées des registres et les alertes de sécurité. Les préposés devraient se familiariser avec les données usuelles et peuvent vérifier les entrées inusitées pour approfondir leurs connaissances.

- **Établir une politique de conservation des registres.** L'information sur un incident peut être consignée en maints endroits. L'élaboration et l'application d'une politique sur la conservation des registres qui précise pendant combien de temps les données des registres doivent être conservées peuvent être très utiles aux fins d'analyse parce que les entrées datant de plus longtemps peuvent faire état d'activités de reconnaissance ou d'attaques similaires antérieures.

- **Corréler les événements.** La preuve relative à un incident peut être consignée dans plusieurs registres. La corrélation des événements à partir de plusieurs sources peut être très utile pour recueillir toute l'information au sujet d'un incident et déterminer si ce dernier s'est effectivement produit.

- **Assurer le synchronisme de toutes les horloges.** Si les horloges des dispositifs servant à signaler les événements ne sont pas synchronisées, la corrélation des événements s'en trouvera compliquée. Les écarts entre les horloges peuvent aussi causer des problèmes de validité de la preuve.

- **Tenir et utiliser une base de connaissances.** Les préposés doivent pouvoir obtenir rapidement de l'information lorsqu'ils analysent un incident. Une base de connaissances centralisée constitue une source d'information cohérente et pouvant être maintenue. Cette base doit comprendre des renseignements généraux, dont des données sur les précurseurs et les indicateurs d'incidents antérieurs.

- **Commencer à consigner toute l'information dès que l'équipe soupçonne qu'un incident s'est produit.** Toutes les mesures prises entre la détection d'un incident et sa résolution finale devraient être documentées et horodatées. Ces renseignements peuvent servir de preuve en cour si des poursuites sont intentées. La consignation des mesures prises peut aussi contribuer au traitement plus efficient et plus systématique du problème et entraîner moins d'erreurs.

- **Protéger les données sur les incidents.** Ces données renferment souvent des informations de nature délicate comme les vulnérabilités, les incidents de sécurité et les cas où des utilisateurs ont pu effectuer des opérations inappropriées. L'équipe doit veiller à ce que l'accès aux données sur les incidents soit adéquatement restreint, tant logiquement que physiquement.

- **Prioriser le traitement des incidents en fonction des facteurs pertinents.** Eu égard aux ressources limitées, les incidents ne doivent pas être traités selon le principe du premier arrivé, premier servi. Les organisations doivent plutôt élaborer des directives écrites qui précisent la rapidité avec laquelle l'équipe doit réagir à l'incident, ainsi que les mesures à prendre, à la lumière de facteurs pertinents tels l'impact de l'incident sur les plans fonctionnel et informationnel et les chances de reprise des activités à la suite de l'incident. Cela permet aux préposés à l'incident d'épargner du temps et de justifier leurs interventions aux yeux de la direction et des responsables des systèmes. Les organisations doivent aussi établir un mécanisme permettant d'acheminer un cas aux échelons supérieurs si l'équipe ne réagit pas à un incident dans le délai prévu.

- **Inclure dans la politique d'intervention en cas d'incident de l'organisation des dispositions sur le signalement des incidents.** Les organisations doivent préciser quels incidents doivent être signalés, à quel moment ils doivent l'être, et qui doit en être informé. Les parties notifiées le plus souvent sont le dirigeant principal de l'information, le chef de la sécurité de l'information, le chef local de la sécurité de l'information, les autres EII de l'organisation et les responsables des systèmes.

- **Établir des stratégies et des procédures pour confiner les incidents.** Il importe de confiner les incidents avec rapidité et efficacité pour en limiter l'impact sur le plan opérationnel. Les organisations doivent définir des risques acceptables pour confiner les incidents, et élaborer des stratégies et des procédures en conséquence. Les stratégies de confinement devraient varier selon le type d'incident.

- **Suivre les procédures établies pour la collecte et le traitement des éléments de preuve.** L'équipe doit clairement documenter la façon dont les éléments de preuve ont été conservés. Il faut pouvoir rendre compte des éléments de preuve à tout moment. L'équipe doit rencontrer le personnel des services juridiques et des organismes d'application de la loi pour discuter du traitement de la preuve, puis élaborer des procédures sur la base de ces discussions.

- **Recueillir en preuve les données volatiles des systèmes.** Cela comprend les listes de connexions réseau, les processus, les séances de connexion, les fichiers ouverts, les configurations d'interface réseau et le contenu de la mémoire. L'exécution de commandes sélectionnées avec soin à partir de supports de confiance permet de recueillir l'information nécessaire sans endommager les éléments de preuve contenus dans le système.

- **Demander à un spécialiste en reconstitution judiciaire d'obtenir des clichés systèmes à l'aide d'images complètes du disque et non de copies de sauvegarde des fichiers.** La plupart des courtiers membres de petite et moyenne taille ne disposent pas des ressources internes nécessaires pour procéder à l'analyse judiciaire d'un système d'information compromis. Il importe de tisser des liens avec un fournisseur local de services de reconstitution judiciaire informatique avant qu'un cyberincident ne survienne. Il importe aussi que le personnel de ce fournisseur ait les accréditations ou les titres de compétence appropriés en criminalistique informatique.

- **Faire le point sur les leçons apprises à la suite d'incidents majeurs.** Les séances permettant de faire le point sur les leçons apprises sont extrêmement utiles pour améliorer les mesures de sécurité et le processus de traitement des incidents lui-même.

Annexe B : Que faire advenant un cyberincident pour lequel on n'est pas préparé

Si un incident de sécurité informatique survient alors que vous ne disposez pas d'un plan d'intervention, exécutez les dix étapes suivantes[xiii] :

Étape 1 – *Restez calme*
Les communications et la coordination se compliquent. Votre attitude calme peut aider les autres à éviter de faire des erreurs critiques.

Étape 2 – *Prenez des notes détaillées*
« Identification des incidents de cybersécurité » À mesure que vous prenez des notes, n'oubliez pas que ces dernières peuvent être déposées en preuve auprès d'un tribunal. Assurez-vous de répondre aux cinq questions suivantes : Qui; Quoi; Où; Pourquoi; et Comment. Un magnétophone que vous pouvez tenir à la main peut être très utile.

Étape 3 – *Prévenez les personnes compétentes et obtenez de l'aide*
Prévenez d'abord votre coordonnateur de la sécurité et votre gestionnaire. Demandez qu'un collègue soit chargé d'aider à coordonner le processus d'intervention en réponse à l'incident. Obtenez copie du répertoire téléphonique de l'entreprise et conservez-le avec vous.

Étape 4 – *Appliquez une politique fondée sur le besoin de savoir*
Transmettez les détails de l'incident au plus petit nombre de gens possible. Rappelez-leur au besoin qu'ils sont considérés comme des personnes de confiance et que l'organisation compte sur leur discrétion. Évitez d'avancer des hypothèses sauf lorsque c'est nécessaire pour décider de la marche à suivre.

Étape 5 – *Utilisez les communications hors-bande*
Si les ordinateurs ont été compromis, ne les utilisez pas pour discuter du traitement de l'incident. Servez-vous plutôt des téléphones et des télécopieurs. Ne transmettez pas de renseignements au sujet de l'incident par courriel. L'auteur de l'incident pourrait intercepter la communication et utiliser l'information pour aggraver la situation. Si vous devez utiliser un ordinateur, assurez-vous d'encrypter tout courriel lié à l'incident.

Étape 6 – *Confinez le problème*
Prenez les mesures nécessaires pour éviter que le problème ne s'aggrave. Vous pourriez notamment devoir isoler le système du réseau.

Étape 7 – *Faites une copie de sauvegarde*
Faites une copie de sauvegarde du ou des systèmes touchés le plus rapidement possible. Utilisez des supports neufs et vierges. Faites une copie binaire ou octet par octet si c'est possible.

Étape 8 – *Éliminez le problème*
Déterminez ce qui a fait défaut si vous le pouvez. Prenez des mesures afin de combler les lacunes qui ont fait en sorte que le problème survienne.

Étape 9 – *Reprenez vos activités*

Après vous être assuré que vos copies de sauvegarde ne sont pas compromises, restaurez votre système à l'aide de ces copies et surveillez-le de près pour déterminer s'il peut reprendre son activité. Suivez le système de près au cours des semaines suivantes pour être certain qu'il ne sera pas compromis à nouveau.

Étape 10 – *Mettez à profit les leçons apprises*
Tirez des leçons de cette expérience pour ne pas être pris au dépourvu la prochaine fois qu'un incident surviendra.

5 Bibliographie

[i] ISACA. *Incident Management and Response*, 2012
[ii] ISO/IEC. ISO 27035-2 (2e ébauche de travail), Information technology - Security techniques - Information security incident management - Part 1: Principles of incident management
[iii] Government of South Australia. *ISMF Guideline 12aCybersecurity Incident Reporting Scheme*, 2014
[iv] Hewlett-Packard. *Executive breach response playbook: How to successfully navigate the enterprise through a serious data breach*, 2015
[v] NIST. *Computer Security Incident Handling Guide*, 2012
[vi] NIST. *Computer Security Incident Handling Guide*, 2012
[vii] NIST. *Computer Security Incident Handling Guide*, 2012
[viii] ISO/IEC. ISO 27035-1 (2e ébauche de travail), *Technologies de l'information -- Techniques de sécurité -- Gestion des incidents de sécurité de l'information*
[ix] Government of South Australia. ISMF Guideline 12a; *Cybersecurity Incident Reporting Scheme*, 2014
[x] Hewlett-Packard. *Executive breach response playbook: How to successfully navigate the enterprise through a serious data breach*, 2015
[xi] Goodwin, Cristin, et J. Paul Nicholas. « A framework for cybersecurity information and risk reduction ». Microsoft, 2015
[xii] Luiijf, E. et Kernkamp, A. *Sharing Cyber Security Information: Good Practice Stemming from the Dutch Public-Private-Participation Approach*, mars 2015
[xiii] Northcutt, Steven. *COMPUTER SECURITY INCIDENT HANDLING: An Action Plan for Dealing with Intrusions, Cyber-Theft, and Other Security-Related Events*, 2003