Guide d'intervention en rançongiciel

Ce document a été conçu à la demande de l'Organisme canadien de réglementation des investissements. Il a pour but de guider la réponse à une attaque par rançongiciel qui peut avoir un impact important sur la continuité des affaires. Il décrit les actions requises pour s'assurer que ces incidents sont traités de manière coordonnée et reproductible. Les procédures doivent être testées et révisées périodiquement au moyen d'exercices basés sur des scénarios.

DATE D'ÉMISSION: 22 août 2023
AUTEUR: Juno Risk Solutions

juno risk solutions

OCRI · CIRO
Organisme canadien de réglementation des investissements
Canadian Investment Regulatory Organization

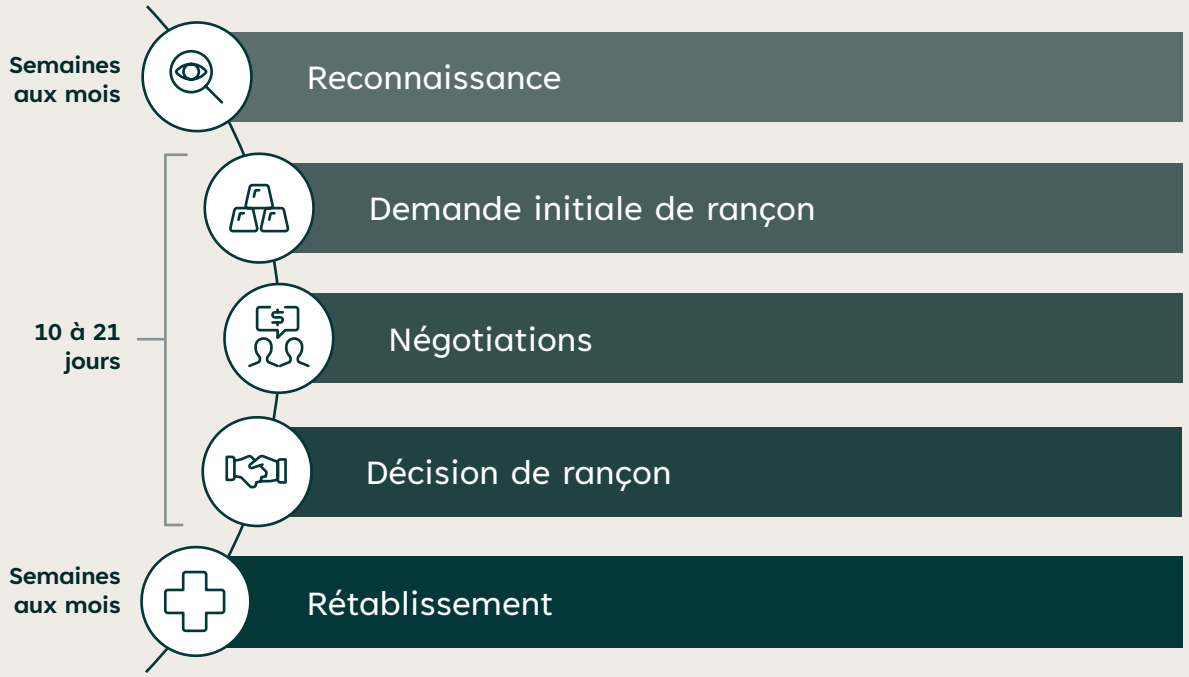
Aperçu des attaques de rançongiciel

Les cyber-incidents sont de plus en plus fréquents et constituent une menace existentielle pour les courtiers en valeurs mobilières et les courtiers en fonds communs de placement canadiens, leurs investisseurs, leurs employés et leurs intervenants. Sans exagération, les cyber-incidents présentent un large éventail de pertes potentielles qui pourraient menacer ces organisations et leurs intervenants. Il est donc essentiel de réagir rapidement, collectivement et efficacement à toute une série de cyberattaques provenant de toutes les facettes de l'entreprise afin de protéger les courtiers en valeurs mobilières et les courtiers en fonds communs de placement canadiens, leurs investisseurs, leurs employés et leurs intervenants. Ces dernières années, des attaques de rançongiciel très médiatisées ont touché le secteur financier canadien, notamment des coopératives de crédit, des compagnies d'assurance et des cabinets d'experts-comptables. Ces attaques ont entraîné d'importantes pertes financières et ont causé des dommages considérables de réputation.

Rançongiciel

Le concept de base d'une attaque par rançongiciel consiste à introduire un logiciel malveillant dans les systèmes informatiques de la cible, à verrouiller ces systèmes, souvent après avoir exfiltré des données sensibles, et à extorquer une rançon en échange d'une clé de décryptage et de la promesse de ne pas divulguer les données volées à des tiers. Les groupes criminels organisés qui mènent des attaques par rançongiciel ont l'intention de créer une série d'impacts - financiers, opérationnels, de réputation, légaux, réglementaires - sur leur cible afin qu'elle soit contrainte de payer la rançon. Les attaques par rançongiciel présentent une série de risques à l'échelle de l'entreprise. Les conséquences qui en découlent se produisent simultanément et ont pour effet de dépasser la capacité de l'entreprise cible à réagir et à gérer la crise. La figure 1 illustre les étapes d'une attaque par rançongiciel et montre que le rétablissement après un incident peut durer des semaines, voire des mois.

Figure 1 – Phases d'attaque de rançongiciel



Risques liés au rançongiciel

Les attaques de rançongiciel sont plus qu'un problème informatique et posent des défis importants et interdépendants aux entreprises. Le tableau 1 met en évidence l'éventail des impacts que les organisations sont susceptibles de subir en cas d'attaque par rançongiciel. Il présente également les protections et les mesures de sauvegarde couramment déployées pour faire face à chacun de ces risques, conformément aux normes de l'industrie. Il est de la responsabilité première des dirigeants de faire face aux risques de manière opportune et coordonnée.

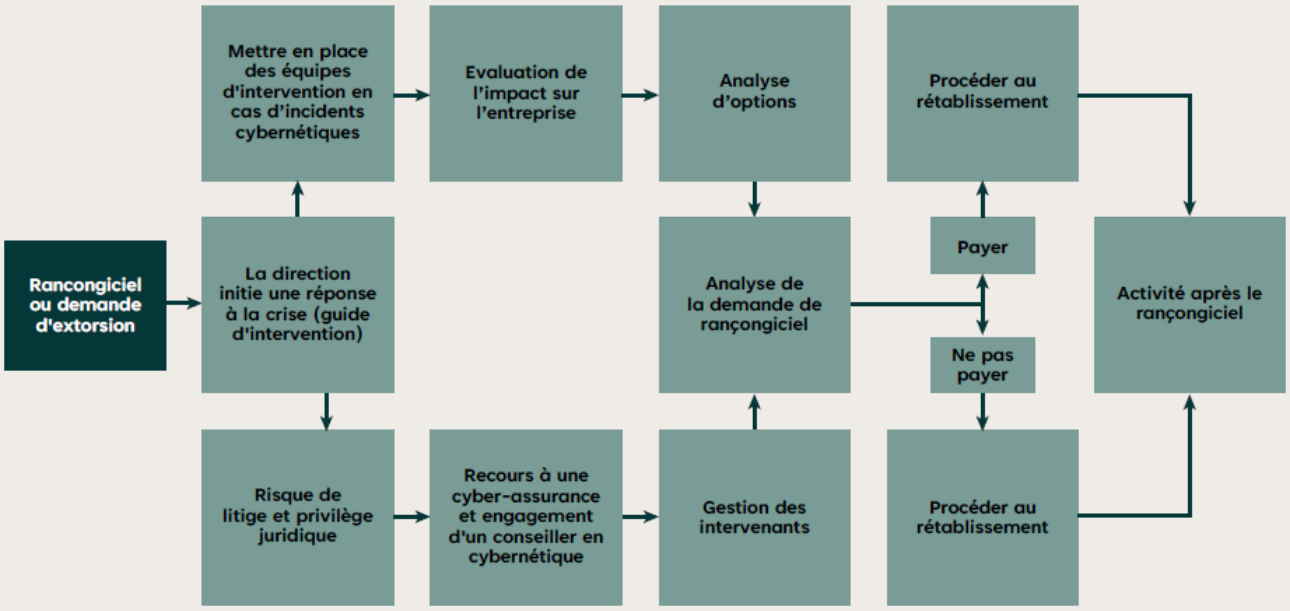
La tâche de l'équipe de direction, de l'équipe de continuité des affaires (dans le cadre d'un plan de continuité des affaires en place), de l'équipe de réponse aux incidents informatiques (dans le cadre d'un plan de reprise après crise), du personnel et du Conseil d'administration d'une organisation est de réagir rapidement et de manière coordonnée. L'effort principal consistera à minimiser les conséquences d'une attaque pour les entreprises, les investisseurs et les intervenants.

Tableau 1 – Risques liés aux cyber-incidents

Risques	Impacts	Réponses
Risque financier	Demande de rançon Pénalités / amendes Perte de revenus / coûts encourus	Réserves financières Assurance cybernétique Émission de la dette
Risque des opérations	Services perturbés Perturbations des systèmes, y compris les sites web et les applications en ligne	Fournisseurs de services tiers Plans de réponse aux incidents Assurance cybernétique Solutions manuelles
Risque de marché	Perturbation des opérations Exposition d'informations personnelles Expérience du client	Plan de communication de crise Assurance cybernétique Procédures de signalement des violations
Risque de réputation	Exposition aux médias Fuite de clients	Plan de communication de crise Assurance cybernétique
Risque réglementaire	Signalement des violations - y compris le signalement multi-juridictionnel au Canada et aux États-Unis Règlements et sanctions	Procédures de signalement des violations Plan de communication de crise
Risque juridique	Litiges Rupture de confidentialité Exigences en matière de notification des contrats	Protocole de privilège juridique Gestion des fournisseurs Assurance cybernétique
Risque lié au capital humain	Épuisement des employés Réduction de la fidélisation des employés Augmentation du taux de démission Incapacité de recruter	Programmes d'aide aux employés Culture d'entreprise Salaires compétitifs Rémunération et avantages concurrentiels

Phases d'attaque de rançongiciel

Figure 2 – Équipes d'intervention en cas d'incident cybernétique



Mesures immédiates à prendre en cas de découverte d'un cyber-incident

Mettre en place des équipes d'intervention en cas d'incident cybernétique

Le rôle de l'équipe de direction lors d'une attaque de rançongiciel est d'agir en tant qu'organe de coordination au plus haut niveau, avec l'autorité de prendre des décisions au nom de l'entreprise. Soutenue par l'équipe de continuité des affaires et l'équipe de réponse aux incidents, qui procèdent à un premier triage de l'incident, recueillent et évaluent les informations et mettent en œuvre les directives de l'équipe de direction, cette dernière prend des décisions stratégiques au nom de l'entreprise et dirige les efforts déployés pour faire face à l'incident. Même les plus petites entreprises disposent de ces fonctions, dont la responsabilité peut incomber à une ou deux personnes seulement au sein de l'organisation.

La première manifestation d'une attaque par rançongiciel sera probablement une forme d'interruption des systèmes informatiques. La réponse initiale à cet événement sera dirigée par l'équipe d'intervention en cas d'incident. L'équipe d'intervention en cas d'incident transmettra l'événement à l'équipe chargée de la continuité des affaires pour un premier triage afin de déterminer si la panne des systèmes a des répercussions qui nécessitent une évaluation plus large à l'échelle de l'entreprise.

Dès la découverte d'une attaque présumée par rançongiciel, l'équipe de direction et l'équipe chargée de la continuité des affaires se réunissent. L'équipe de continuité des affaires présentera à l'équipe de direction son triage de l'incident et une première évaluation des conséquences de l'incident.

Figure 3 – Équipes d'intervention en cas d'incident cybernétique

Risque de litige et privilège juridique

Toute perturbation majeure des services doit d'abord être évaluée afin de déterminer si l'événement introduit la possibilité d'une action en justice. Tous les incidents ne présentent pas ce risque. Cependant, tout incident lié à un rançongiciel ou à une violation de données présente un risque de litige. Lors du triage initial de l'incident par l'équipe de continuité des affaires, le conseiller juridique de l'organisation déterminera si l'incident présente un risque d'action en justice. Si le conseiller juridique détermine qu'il existe un risque de litige, il demandera que l'incident soit géré sous le couvert du privilège juridique.

Le secret professionnel permet à une organisation de communiquer librement avec ses avocats au sujet d'un cyber-incident afin d'obtenir un avis juridique franc, sans craindre que ces communications et les documents connexes soient divulgués à d'autres personnes, y compris dans le cadre d'un litige. Il permet également aux avocats d'une organisation de prendre des mesures pour défendre l'organisation dans le cadre d'un litige ou en prévision d'un litige, sans craindre que les notes de l'avocat ne soient divulguées à d'autres personnes et utilisé contre leur client. La gestion de la réponse aux incidents par le directeur juridique, sous le couvert du secret professionnel, est une étape essentielle pour protéger l'organisation en cas d'action en justice.

Invocation de l'assurance cybernétique et l'engagement d'un conseiller en cybercriminalité

Si une organisation subit une attaque de rançongiciel réelle ou raisonnablement suspectée, elle doit immédiatement en informer son fournisseur d'assurance cybernétique ou son courtier d'assurance si l'organisation a souscrit une assurance cybernétique. La cyber-assurance offre généralement une couverture pour les interventions en cas de violation qui donne accès à un panel de fournisseurs de services experts en la matière. Il s'agit notamment d'un conseiller en cybernétique, un expert spécialisé dans la gestion des cyber-incidents, qui fournit des conseils juridiques précieux et une assistance dans la gestion des efforts de réponse. Le rôle du conseiller en cybernétique consiste essentiellement à agir en tant que chef de projet spécialisé dans les cyber-incidents. Le conseiller en cybernétique fera appel aux fournisseurs de solutions de crise prévus par la cyber politique et fournira ces ressources sous le couvert du secret professionnel.

Évaluation des impacts sur l'entreprise

Les entreprises s'appuyant de plus en plus sur la technologie, il est essentiel qu'elles adoptent une approche globale de la gestion des risques. Cela est particulièrement vrai en ce qui concerne les attaques par rançongiciel, car elles ne menacent pas seulement la technologie, mais ont également des répercussions sur l'ensemble de l'entreprise. Pour aider l'équipe de direction à mieux comprendre, au niveau de l'entreprise, les conséquences générales d'un cyber-incident, le tableau 2 présente un cadre d'évaluation de haut niveau de l'impact basé sur le risque. L'objectif de ce cadre est de saisir l'éventail des conséquences potentielles et en temps réel auxquelles l'organisation peut être confrontée lors d'un cyber-incident, y compris les perturbations des principales lignes d'activité, les incidences financières et les atteintes à la réputation.

Tableau 2 - Cadre d'analyse d'impact basé sur les risques

	Jour 1	Jour 7	Jour 14	Jour 21	Jour 28
Impact inancier					
Impact sur les revenus					
Revenus perdus ou différés					
Dépenses encourues ou coûts d'opportunité					
Risques lies aux comptes clés					
Couts encourus					
Coûts d'intervention					
Coûts de rétablissement					
Risque de litige					
Violation des données					
Demande de la rançon					
Rançon					
Impact opérationnel					
Services différés					
Transactions perturbées					
Impact de réputation					
Médias traditionnels et sociaux					
Intervenants					
Action juridique					
Embarras du leadership					
Mandat					

Ce cadre d'évaluation fondé sur les risques devrait être pris en charge par l'équipe de continuité des affaires de l'organisation et soutenu par l'équipe de réponse aux incidents, qui fournit une analyse des impacts financiers, opérationnels et de réputation présentés par un cyber-incident en temps réel, ainsi que des projections pour les semaines à venir. Cette évaluation est utilisée pour fournir à l'équipe de direction la connaissance de la situation nécessaire pour prendre des décisions en connaissance de cause. Lorsqu'elle examine le cadre d'évaluation fondé sur les risques, l'équipe de direction doit déterminer avec soin quelles sont les conséquences de l'incident cybernétique qui justifient la plus grande priorité des efforts de réponse.

Ce cadre permet à l'équipe de direction de prendre en compte l'ensemble des conséquences pour l'entreprise et de décider en connaissance de cause s'il convient ou non de payer la rançon.

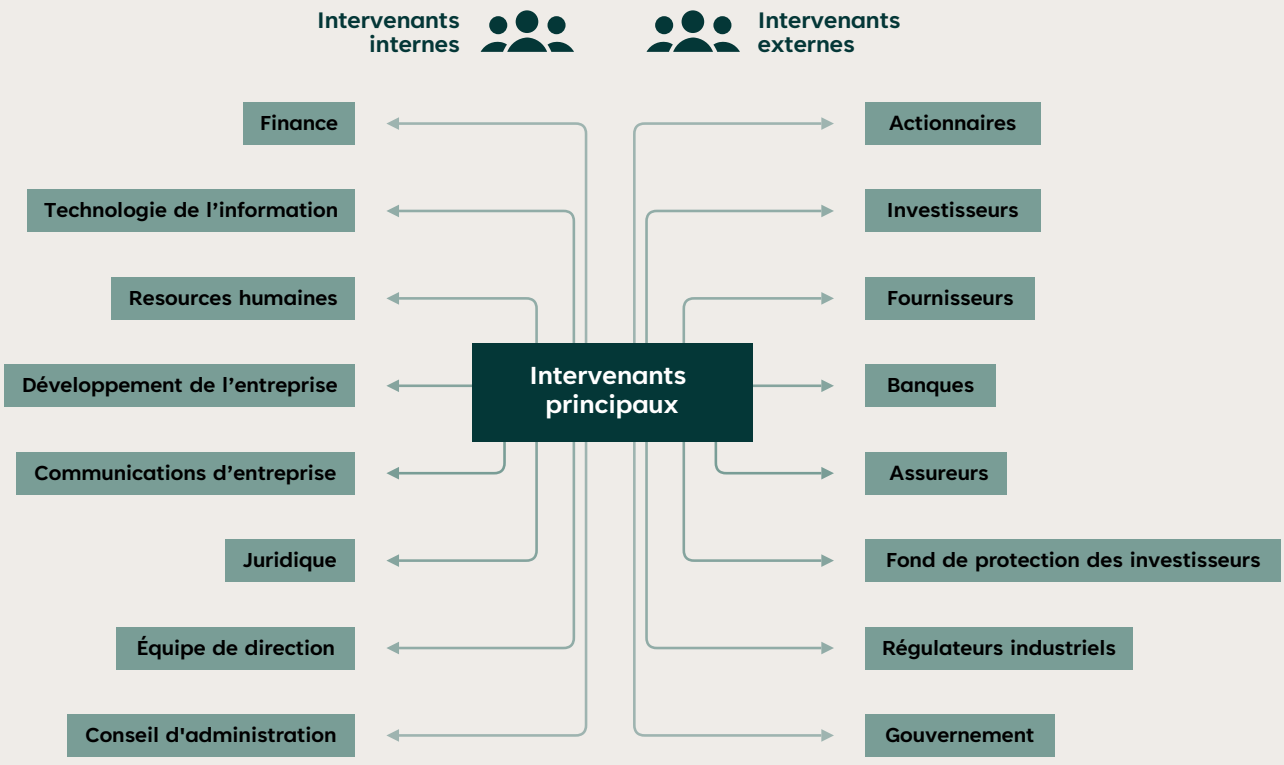
Gestion des intervenants

La figure 4 présente les principaux intervenants pour les courtiers en fonds d'investissement ou les courtiers en fonds communs de placement. Il est essentiel que les communications soient gérées avec soin pour les intervenants internes et externes.

Une attaque par rançongiciel crée deux tensions opposées au sein d'une organisation :

- La nécessité d'informer immédiatement les clients et les autres intervenants directement touchées par des messages précis et appropriés ; et
- L'obligation de protéger les informations confidentielles relatives à la réponse à l'incident contre toute diffusion involontaire, ce qui augmenterait les risques de litige.

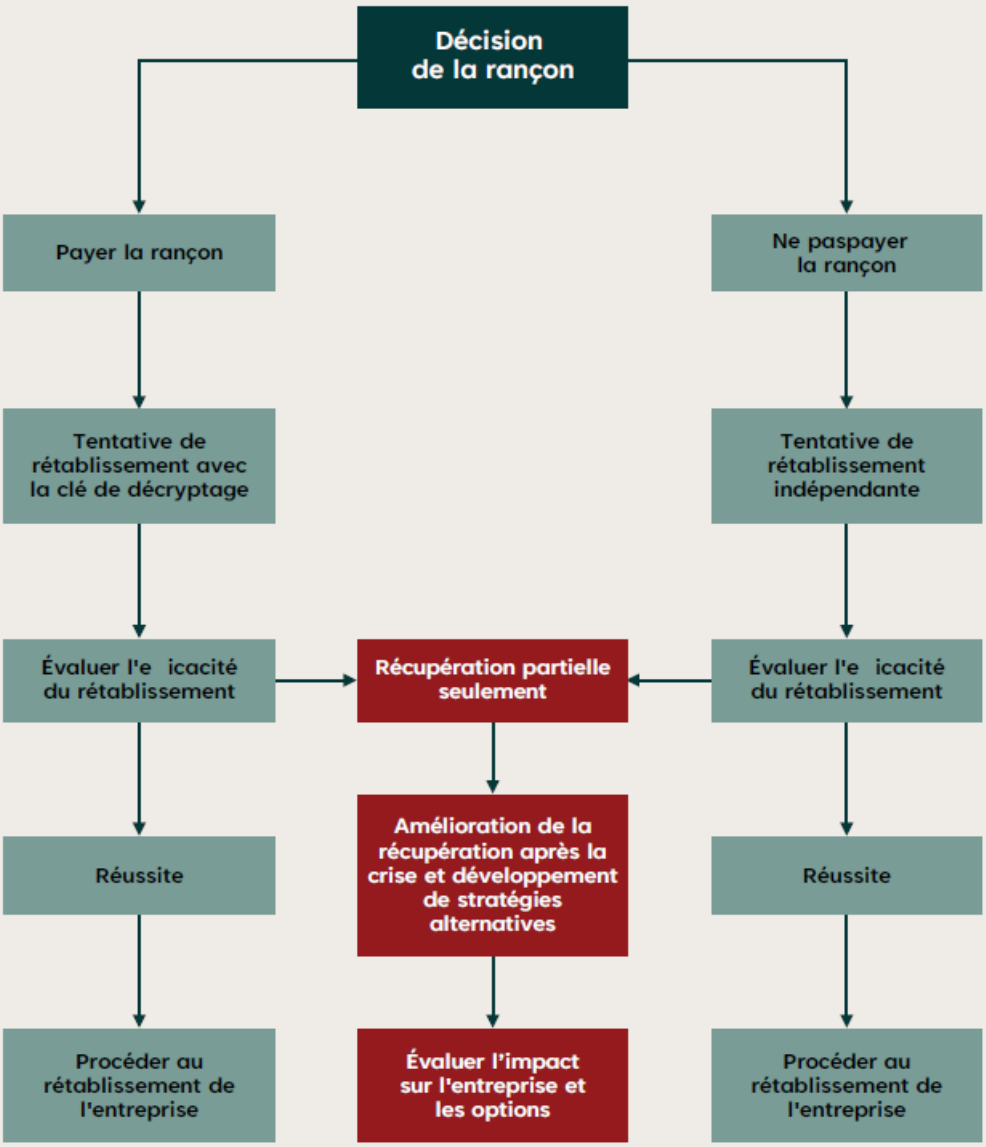
Figure 4 – Intervenants principaux



Analyse d'options

Une attaque par rançongiciel offre à l'équipe de direction une série d'options à différents phases de la crise. La figure 5 met en évidence les points de décision de l'équipe de direction en cas de cyber-incident et souligne que l'équipe de direction doit être bien informée par l'équipe de continuité des affaires et l'équipe d'intervention en cas d'incident pour faciliter la prise de décision. Chaque point de décision nécessite l'examen de l'éventail des options présentées à l'équipe de direction en ce qui concerne la capacité de l'organisation à surmonter la crise, la confiance suffisante dans les capacités de rétablissement et l'urgence de la prise de décision.

Figure 5 – Modèle d'analyse d'options



Analyse de la demande de rançon

Considérations sur l'impact des risques

Prendre la décision de payer une rançon à un acteur criminel n'est pas chose aisée. Elle soulève des questions émotionnelles quant à la possibilité de payer une rançon qui, en fin de compte, récompense les criminels. Cependant, une attaque par rançongiciel présente une série de risques pour l'entreprise, qui doivent tous être pris en compte lorsqu'il s'agit de décider de la manière de répondre à une demande de rançon.

Tandis que l'équipe chargée de la continuité des affaires et l'équipe chargée de la réponse aux incidents continuent d'invoquer leurs plans respectifs de réponse aux incidents, l'équipe de direction doit élaborer et mettre en œuvre des stratégies visant à éradiquer la cybermenace. L'équipe de direction doit tenir compte de l'éventail des conséquences de l'incident cybernétique sur l'organisation. Le tableau 3 présente les considérations générales à prendre en compte pour toute une série de vecteurs d'impact.

Tableau 3 – Considérations sur l'impact des risques

Financier	• L'impact financier de l'incident cybernétique sur l'entreprise est-il durable ? • À quel moment la charge financière peut-elle dépasser la demande de rançon ? • L'équipe de direction a-t-elle le pouvoir de faciliter le paiement d'une rançon ?
Opérationnel	• Comment les normes de niveau de service sont-elles gérées ? • Quelle est l'ampleur de l'arriéré de transactions non traitées et combien de temps faudra-t-il pour récupérer ces transactions et ramener l'entreprise à un rythme opérationnel normal ?
Réglementation	• En cas de violation de données, l'organisation a-t-elle l'obligation de prendre des mesures pour protéger les informations personnelles identifiables (IPI) violées contre toute divulgation ultérieure ? • Le paiement d'une rançon en échange de la restitution ou de la destruction de ces informations permettrait-il de mieux s'acquitter de cette obligation ?
Réputation	• Quel est l'impact sur la réputation de l'organisation de l'interruption continue des opérations ? • Quel est l'impact sur la réputation d'une divulgation totale ou partielle des données volées de l'entreprise ? • Quel est l'impact sur la réputation si l'organisation décide de payer la rançon et que ces informations sont rendues publiques ?
Sanctions	• L'acteur de la menace est-il connu du conseiller en cybernétique et de son équipe ? • L'acteur de la menace qui a mené la cyberattaque fait-il l'objet de sanctions au Canada ou dans une autre juridiction qui présente un risque réglementaire si l'acteur de la menace est payé ?
Impact sur le personnel	• Quelle est la nature du risque que la crise fait peser sur le capital humain ? • Quelle sera la réaction du personnel si l'entreprise décide de payer ou non la rançon ? • Combien de temps l'organisation peut-elle continuer à gérer efficacement le stress du personnel et de la direction ?
Retour aux opérations	• Dans quelle mesure est-il impératif que l'organisation reprenne rapidement ses activités ? • Les risques commerciaux évalués donnent-ils à l'organisation le temps de continuer à négocier ou de tenter de reprendre ses activités de manière indépendante sans payer la rançon ?

Rétablissement d'entreprise

Évaluation du processus de rétablissement

La capacité de l'organisation à répondre à un incident, à le gérer et à s'en remettre peut réduire de manière significative les pertes financières, opérationnelles et de réputation. L'équipe de direction, l'équipe de continuité des affaires et l'équipe de réponse aux incidents disposent de leviers - mis en évidence tout au long de ce guide d'intervention et inclus dans les plans de réponse aux incidents - qui peuvent directement influencer les résultats de l'incident. L'utilisation de ces outils peut conduire à des résultats positifs, tandis qu'une utilisation limitée peut avoir des conséquences négatives.

Surveillance du processus de rétablissement

La priorité en cas de cyber-événement est de résoudre les problèmes immédiats qui affectent les systèmes, les données et les opérations qui facilitent les services essentiels. L'équipe de direction doit demander à l'équipe chargée de la continuité des affaires et à l'équipe chargée de la réponse aux incidents de prendre les mesures nécessaires pour rétablir les services essentiels et de surveiller en permanence les efforts de rétablissement jusqu'à ce que la crise puisse être levée. La figure 6 présente un tableau de bord de haut niveau pour la reprise des activités afin d'assurer la supervision nécessaire des activités de réponse.

Une fois les conséquences immédiates de la crise résolues, l'équipe de direction doit veiller à ce que l'organisation reprenne ses activités normales. De nombreuses organisations victimes d'un cyber-incident ne se rétablissent jamais complètement. Une fois que l'organisation a désamorcé la réponse à la crise en gérant les priorités immédiates à court terme, l'accent mis sur le rétablissement est perdu et l'organisation ne parvient pas à retrouver les niveaux d'avant l'incident.

Il est important qu'au fur et à mesure que l'organisation poursuit le rétablissement des services essentiels par le rétablissement des systèmes, des données et de l'opérabilité, l'accent soit mis sur le rétablissement financier, la gestion de la confiance des intervenants et le rétablissement de la réputation. Ces attributs sont plus difficiles à mesurer, mais ils ont le plus grand impact à long terme sur l'organisation.

Figure 6 – Fiche de suivi de rétablissement

Rétablissement de:	Semaine			
	1	2	3	4
Systèmes	*Critères, objectifs clés & indicateurs de performance clés*			
Données				
Opérations				
Confiance des parties intéressées				
Financier				

Légende	Dépassement de l'objectif	Objectif atteint	À risque	Inacceptable	Très inacceptable

Activité après l'incident

Analyse de l'après-crise

Après l'incident, les organisations doivent saisir l'occasion d'enquêter sur les causes de la crise, en recherchant et en agissant sur les preuves de problèmes culturels plus larges qui pourraient en être à l'origine, et en identifiant les possibilités de changement pour acquérir un avantage concurrentiel et une plus grande résilience.

Renforcement des défenses - Une fois l'événement terminé, l'organisation doit immédiatement prendre des mesures pour minimiser la probabilité qu'il se reproduise. Parmi les entreprises qui ont signalé une cyberattaque entre 2021 et 2022, nombreuses sont celles qui ont déclaré avoir subi plus d'une attaque. Compte tenu de la publicité qui accompagne une cyberattaque, on peut supposer que l'organisation présente une certaine forme de vulnérabilité qui a permis l'attaque initiale. Le fait de ne pas remédier à cette vulnérabilité initiale peut conduire à une nouvelle attaque.

Rapports réglementaires - Des rapports réglementaires, y compris des rapports sur les infractions, peuvent être exigés. Dans certaines juridictions, dans le cas où un attaquant de rançongiciel exfiltre des données et prétend les avoir détruites dans le cadre de la négociation de la rançon, une entreprise peut toujours avoir besoin de faire un rapport de violation s'il n'y a pas de preuve concrète que les données ont été détruites.

Rapport après action - Documenter la façon dont l'organisation a réagi à la crise et la meilleure façon d'améliorer les réactions en cas d'événements futurs.

Ce processus doit également être dirigé par le directeur juridique en vertu du secret professionnel.

Gestion des clients - S'engager auprès des clients clés et des tiers pour gérer les relations afin d'éviter la fuite des clients et les atteintes à la réputation à long terme.

Plans de crise - Examiner les plans de crise, les processus et les compétences pour déterminer :

- Les processus ont-ils fonctionné et l'information a-t-elle bien circulée ?
- La communication avec les intervenants était-elle adéquate et opportune ?
- Les plans ont-ils été correctement préparés avant la crise pour aider à sa gestion ?
- Les exigences réglementaires ont-elles été prises en compte avec précision et en temps voulu ?

Apprentissages tirés - L'équipe de direction doit veiller à ce que l'équipe chargée de la continuité des affaires et l'équipe d'intervention en cas d'incident entreprennent une enquête sur les apprentissages tirés après la crise, sous la direction d'un cadre supérieur ayant l'expérience requise. Les domaines clés de ce processus doivent inclure une évaluation de la nature de la menace à laquelle l'organisation est confrontée, l'efficacité des mesures de réponse à l'incident de l'organisation et une évaluation du rôle du Conseil d'administration dans la réponse à la crise.