ANNEXE – *Contexte de la cueillette de renseignements sur les cyberincidents par les forces de l'ordre*

Soutien aux enquêtes sur la cybercriminalité – Questions des forces de l'ordre aux victimes

Objectif

Dès le début de la cueillette de renseignements à l'aide de ces questions, l'agent d'application de la loi qui pose les questions et le plaignant qui signale l'incident comprendront tous les deux l'objectif sous-jacent de cette collaboration. Ce questionnaire est le fruit de consultations et d'importantes contributions de spécialistes de la cybersécurité évoluant au sein de services policiers ou juridiques qui interviennent régulièrement dans des cas de cyberincidents. L'objectif est le suivant : *permettre à l'agent d'application de la loi de recueillir des renseignements sur une possible infraction criminelle contre une victime de cybercriminalité. Les renseignements sont demandés pour appuyer la réduction de la cybercriminalité et pour permettre aux ressources de fournir du soutien aux victimes. Ils ne sont aucunement demandés pour accéder à des renseignements qui seraient assujettis à un privilège. L'objectif énoncé sera atteint des façons suivantes et aux fins suivantes :*

1. *détermination des personnes soupçonnées de mener des activités criminelles qui ciblent les cybersystèmes dont dépendent les victimes;*
2. *cueillette d'éléments de preuve contre les criminels présumés afin de procéder à d'éventuelles arrestations, mises en accusation et poursuites;*
3. *obtention de renseignements susceptibles de contribuer aux activités d'application de la loi visant à perturber les activités cybercriminelles actuelles et futures;*
4. *pour appuyer tous les processus d'application de la loi et de poursuites judiciaires contre des cybercriminels;*
5. *pour permettre aux forces de l'ordre de bien appuyer les victimes de cybercriminalité lorsqu'elles ont besoin d'aide et favoriser la création de liens entre les victimes et les ressources et services susceptibles de les aider.*

Renseignements essentiels requis par les forces de l'ordre

Au début de collaboration entre l'enquêteur et la victime, il est possible que la victime hésite à fournir les renseignements demandés par les forces de l'ordre. C'est peut-être parce qu'elle ne sait pas exactement en quoi consistera l'enquête sur le criminel en question. C'est peut-être aussi parce qu'à un certain moment durant le processus d'intervention à la suite du cyberincident, le risque de communication des renseignements compromis à toute personne de l'extérieur, y compris aux forces de l'ordre, a été évalué. Quelle que soit la raison, il est bon de transmettre le document intitulé *À QUOI S'ATTENDRE AU DÉBUT D'UNE ENQUÊTE SUR LA CYBERCRIMINALITÉ* au début du processus de collaboration avec la victime, avant même qu'elle rencontre l'enquêteur pour la première fois.

Afin de garantir une transparence complète, les organisations victimes et les personnes qui signalent des cyberincidents aux organismes d'application de la loi doivent comprendre quels renseignements ces derniers cherchent à obtenir. Les renseignements demandés relativement au cyberincident visent à garantir que les parties qui participent à l'enquête, à la poursuite et/ou à l'intervention à la suite de l'incident sont en mesure d'exécuter leurs tâches et leurs fonctions.

Ces renseignements appuient les activités des organismes d'application de la loi pour intenter des poursuites contre les criminels et ne doivent pas être assujettis à un privilège. Voici certains des renseignements essentiels de base qui sont obtenus au moyen de ce questionnaire :

1. identification de l'organisation victime et renseignements contextuels;
2. faits relatifs à l'incident et gravité des répercussions associées, y compris le nombre de terminaux touchés et d'autres facteurs;
3. vecteurs de l'attaque;
4. comptes et attributions de l'auteur de menace;
5. adresses et activités de monnaie virtuelle clés liées à l'incident;
6. fichiers journaux pertinents sur le réseau/l'hôte;
7. indicateurs de compromission et autres tactiques, techniques et procédures observées.

Processus pour la fourniture des renseignements

Les *questions des forces de l'ordre sur le cyberincident* sont fondées sur une approche en deux étapes pour la fourniture de renseignements par l'organisation victime. Les forces de l'ordre se serviront de ce questionnaire pour obtenir des renseignements dans le cadre d'un processus de collaboration en deux étapes fiable et respectueux des victimes.

La première étape consistera en six questions concises visant à recueillir les renseignements les plus importants et les plus urgents dont les forces de l'ordre ont besoin pour faire une intervention appropriée.

La deuxième étape consistera à recueillir des renseignements de suivi plus détaillés et/ou des renseignements expliquant davantage le contexte de l'incident.

Il est possible que les renseignements demandés aux deux étapes soient recueillis en même temps si les ressources le permettent et si le plaignant est disponible lors de la rencontre initiale. En règle générale, les renseignements demandés à la deuxième étape sont recueillis lors de suivis au fur et à mesure que l'incident progresse, en fonction de la disponibilité du plaignant et des renseignements et selon l'évolution de l'incident.

Renseignements sur le signalement, première étape

1. ***Renseignements sur le plaignant ou la personne qui signale l'incident***
   But : la personne ou l'organisation qui signale l'incident s'identifie, fournit les coordonnées d'une personne-ressource principale pour le suivi et explique son lien avec le cyberincident (p. ex. le nom du plaignant, son titre ou son poste/lien avec la victime, ses coordonnées).

2. ***Renseignements sur la victime de l'incident***
   But : la personne qui signale l'incident identifie l'organisation victime et fournit des renseignements connexes pour aider les forces de l'ordre à évaluer des questions comme le territoire de compétence et la coordination requise, le cas échéant, avec d'autres organismes

d'application de la loi (p. ex. le nom de l'organisation, son adresse, ses fonctions principales ou les principaux services offerts, ainsi que d'autres renseignements contextuels, s'il y a lieu, comme le secteur/sous-secteur des infrastructures essentielles, la structure organisationnelle et les emplacements géographiques connexes, le cas échéant).

3. ***Renseignements clés décrivant l'incident***

But : les renseignements demandés visent à fournir des éléments contextuels importants pour comprendre le type d'incident qui s'est produit, de même que son ampleur, sa portée et ses répercussions. Ces renseignements fournissent des détails sur le type d'activité criminelle qui a été commise et des éléments importants relatifs à la gravité du crime. Ces détails peuvent aussi fournir des renseignements contextuels utiles qui pourraient permettre d'établir des liens avec des activités criminelles antérieures. À ce stade, certains de ces renseignements pourraient être des renseignements confidentiels de l'organisation victime et cette dernière doit pouvoir décider quels sont ceux qu'elle est à l'aise de communiquer. Si les forces de l'ordre ont besoin de certains renseignements pour pouvoir régler des problèmes de sécurité publique d'intérêt immédiat, l'agent d'application de la loi doit en informer la victime et lui présenter le contexte de cette demande.

Voici quelques exemples :

   a. ***aperçu de l'incident :*** *renseignements préliminaires (c.-à-d. renseignements connus à ce jour) sur ce qui s'est produit (p. ex. fuite de données, rançongiciel, attaque par déni de service) et détails sur les éléments touchés;*
   b. ***description générale des activités touchées par l'incident :*** *aperçu général, selon le niveau de précision déterminé par l'organisation, pouvant comprendre une description des services ou le nombre d'employés touchés, l'ampleur des répercussions et les services toujours entièrement disponibles au moment du signalement;*
   c. ***chronologie de l'incident :*** *renseignements préliminaires, comme les principaux points de la chronologie de l'incident, qui peuvent être communiqués à cette étape (p. ex. moment où l'incident a été découvert pour la première fois, évolution de l'incident et état actuel);*
   d. ***répercussions connues de l'incident :*** *évaluation initiale du niveau de menace des répercussions, selon les renseignements que l'organisation victime est prête à communiquer à ce stade. Ce qui compte le plus pour les forces de l'ordre maintenant, c'est de déterminer s'il y a un risque connu pour la sécurité publique et/ou un risque actuel ou prévu pour les infrastructures essentielles (répercussions négatives sur la sécurité publique, les finances de l'organisation, l'économie régionale ou nationale, les services essentiels, répercussions en aval sur les clients ou la chaîne d'approvisionnement, etc.)*

4. ***Renseignements sur l'auteur de la menace***

But : les renseignements recueillis visent à fournir aux forces de l'ordre des détails qui pourraient lui permettre d'établir un lien entre l'incident et d'autres activités criminelles de l'auteur de la menace ciblant la victime. Il convient de souligner que des renseignements plus techniques ou plus détaillés seront recueillis à la deuxième étape. Les renseignements recueillis à la première

étape sont des renseignements préliminaires qui peuvent aider les forces de l'ordre à déterminer s'il y a un danger immédiat associé à un incident en cours.

Il peut s'agir, par exemple, de toute communication directe, passée ou actuelle, avec l'auteur de la menace jusqu'au moment du signalement.

5. ***Autres renseignements sur l'incident qui n'ont pas encore été fournis***
   But : tous les renseignements relatifs à l'incident sont importants, même si le plaignant ou la victime peut ne pas le croire au départ. Par exemple, y a-t-il à ce stade d'autres renseignements susceptibles d'aider les forces de l'ordre à mieux comprendre l'incident?

6. ***Coordonnées de la personne-ressource principale***
   But : selon les renseignements recueillis à la première étape du signalement, les forces de l'ordre pourraient faire un suivi afin d'obtenir plus de détails pour appuyer une enquête criminelle ou d'autres activités d'application de la loi qui pourraient être associées au cyberincident signalé. L'organisation victime doit fournir les coordonnées d'une personne-ressource principale avec qui les forces de l'ordre pourront faire un suivi et discuter de l'incident de manière plus approfondie. Il peut s'agir d'une personne qui appuie le processus d'intervention en cas d'incident dans une organisation externe publique ou privée, p. ex. dans un cabinet d'avocats (y compris un conseiller en matière d'atteinte à la vie privée), une compagnie d'assurance, une banque, une équipe d'intervention en cas d'incident informatique ou le Centre canadien pour la cybersécurité.

Renseignements sur le signalement, deuxième étape

1. ***Renseignements sur l'intervention à la suite de l'incident***
   But : les renseignements recueillis visent à avoir plus de détails, possiblement plus techniques, que ceux fournis à la première étape (section 3, renseignements clés décrivant l'incident). Comme pour l'étape précédente, certains renseignements pourraient être des renseignements confidentiels et les forces de l'ordre doivent en tenir compte et expliquer pourquoi ces renseignements sont utiles à l'enquête, qu'ils seront utilisés dans ce contexte seulement et qu'ils ne seront en aucun cas divulgués au public. Il est fort probable que certains aspects du crime commis contre la victime correspondent à des tactiques, des techniques ou des procédures utilisées contre d'autres victimes. Les renseignements demandés pourraient aider les forces de l'ordre à établir des liens avec d'autres administrations dans la poursuite des acteurs malveillants. Les renseignements demandés à cette étape pourraient comprendre, s'ils sont disponibles, les suivants :
   - ***a.*** *renseignements plus précis sur la chronologie de l'incident et l'ampleur de la compromission;*
   - ***b.*** *renseignements connus à ce jour concernant l'intrusion, y compris les indicateurs de compromission, ainsi que les tactiques, les techniques et les procédures utilisées aux fins d'accès et d'infiltration;*
   - ***c.*** *fichiers journaux pertinents sur le réseau liés à l'incident;*
   - ***d.*** *rapport préliminaire sur l'intervention à la suite de l'incident (si disponible).*

2. ***Renseignements sur l'auteur de la menace***
But : les renseignements recueillis visent à fournir aux forces de l'ordre des détails qui pourraient lui permettre d'établir un lien entre l'incident et d'autres activités de l'auteur de la menace ciblant la victime. Dans certains cas, surtout si la victime est toujours en communication avec l'auteur de la menace, certains renseignements pourraient apporter une valeur corrélée immédiate en permettant aux forces de l'ordre de transmettre à l'organisation victime des détails sur l'intervention ou les mesures d'atténuation, afin qu'elle en tienne compte dans son processus d'intervention à la suite de l'incident.

Il peut s'agir, par exemple, de communications avec l'auteur de la menace, comme des renseignements relatifs à la compromission de courriers électroniques professionnels, à l'hameçonnage ou à des demandes de rançon. Ces renseignements pourraient notamment comprendre les suivants :

- **a.** auteurs de l'attaque;
- **b.** communications et/ou transactions avec l'auteur de la menace;
- **c.** comptes et attributions associés à l'auteur de la menace;
- **d.** adresses et activités de monnaie virtuelle clés liées à l'incident.

3. ***Renseignement sur un incident de rançongiciel***
Il convient de souligner qu'une organisation victime peut parfois hésiter à faire appel aux forces de l'ordre dans le cas d'un incident impliquant le versement d'une rançon. L'agent d'application de la loi qui intervient doit être sensible à cette question et se montrer rassurant quant au fait que, bien que les forces de l'ordre n'appuient pas le versement de rançons aux cybercriminels, car cela encourage les activités cybercriminelles, elles reconnaissent que l'organisation victime a le droit de gérer les risques liés à la continuité de ses activités et de prendre des décisions en conséquence. Les renseignements fournis concernant la communication avec l'auteur de la menace et tout renseignement connexe lié au versement d'une rançon ne seront jamais utilisés contre la victime, mais uniquement pour appuyer l'enquête contre l'auteur du cybercrime. Les renseignements demandés pourraient comprendre les suivants :

- ***a.*** *Autres artéfacts de données liés à l'incident (p. ex. notes de rançon, numéros d'identification de porte-monnaie bitcoin, courriels, sobriquets, appels téléphoniques, adresses IP suspectes, fichiers malveillants, fichiers journaux, etc.)*
  (REMARQUE : le fait que l'emplacement des fichiers soit correctement indiqué [endroit où il se trouve dans l'ordinateur, nom, chemin d'accès au fichier et date de création] facilitera le travail; ces informations, si elles sont disponibles, seront très utiles dans le cadre des activités d'application de la loi.)
- ***b.*** *Une rançon a-t-elle été versée?*
  - ***i.*** *Si oui, tous les renseignements associés au paiement, y compris les adresses et activités de monnaie virtuelle clés liées à l'incident.*
  - ***ii.*** *Si l'organisation envisage de verser la rançon, les renseignements sur le processus associé à la transaction à venir.*
    (Remarque : les forces de l'ordre n'ont pas besoin de savoir pourquoi l'organisation a décidé de verser ou non la rançon.)

4. ***Autres renseignements sur l'incident qui n'ont pas encore été fournis***
   But : tous les renseignements relatifs à l'incident sont importants, même si le plaignant ou la victime peut ne pas le croire au départ. Y a-t-il à ce stade d'autres renseignements susceptibles d'aider les forces de l'ordre à mieux comprendre l'incident?