

Guide de sécurité des TI
Publication de l'organisme conseil G2-008



Informatique judiciaire :

Guide à l'intention des intervenants en cas
d'incident de sécurité informatique

Sous-direction de la sécurité technique
Opérations techniques
Gendarmerie royale du Canada
Publié : mai 2008

Dégagement de responsabilité

La présente publication a été préparée par la GRC à l'intention du gouvernement fédéral. Elle est officieuse et d'envergure limitée. Il ne s'agit pas d'une évaluation ni d'une approbation de technologie par la GRC. Elle représente l'opinion de la GRC formulée en fonction de l'information disponible au moment de sa rédaction. La responsabilité de toute utilisation du présent document ou de toute décision prise fondée sur ce dernier par un tiers lui revient. La GRC se dégage de toute responsabilité à l'égard des dommages que pourrait subir un tiers découlant des décisions ou des actions fondées sur la présente publication.

©Tous droits réservés 2008 Gouvernement du Canada, Gendarmerie royale du Canada (GRC)
1200, promenade Vanier, Ottawa (Ontario) Canada K1A 0R2

La présente publication peut être reproduite intégralement sans frais à des fins éducatives et personnelles seulement. Toutefois, l'autorisation écrite de la GRC est requise pour utiliser ce document sous forme révisée ou d'extraits, ou à des fins commerciales.

TABLE DES MATIÈRES

1	Introduction	1
1.1	Objectif.....	2
1.2	Hypothèses.....	2
2	Aperçu du problème.....	2
3	Meilleures pratiques.....	3
3.1	Règlement d'un incident et intervention.....	3
3.2	Détection des incidents de sécurité informatique	3
3.3	Participation des organismes d'application de la loi	4
3.3.1	Mesures qui précèdent l'application de la loi.....	5
3.3.2	Communication avec les organismes d'application de la loi	6
3.4	Aspects juridiques.....	7
3.4.1	Preuve	7
3.4.2	Règles de preuve	7
3.4.3	Chaîne de possession.....	8
4	Conclusion	9

1 Introduction

Les incidents de sécurité informatique et les délits informatiques sont de plus en plus fréquents en milieu de travail. Chaque année, les organismes d'application de la loi sont appelés à résoudre de tels incidents. Cependant, les incidents informatiques ne sont pas tous des crimes. En principe, le personnel ministériel de la sécurité des technologies de l'information (TI) du gouvernement du Canada devrait gérer tous les incidents de sécurité informatique qui sont considérés comme des violations de la politique du ministère sur la sécurité. Lorsque l'incident est, ou semble être, de nature criminelle, les ministères et organismes fédéraux doivent consulter les organismes d'application de la loi le plus tôt possible. Toutefois, comme la priorité des responsables de l'application de la loi est le crime, il est dans l'intérêt de toutes les parties touchées que les ministères soient raisonnablement certains qu'un crime a été commis avant de le signaler.

Dès qu'un comportement suspect ou un incident est décelé, les intervenants en cas d'incident de sécurité informatique doivent être prêts à réagir rapidement et efficacement à la situation afin de limiter les dommages, de communiquer la situation aux parties compétentes, de prendre les mesures de prévention qui s'imposent, de rétablir le service visé et, enfin, d'effectuer un examen après l'incident pour vérifier l'efficacité des procédures et des processus d'intervention en vigueur. En vue de faciliter une intervention adéquate en cas d'incident de sécurité informatique, il convient de documenter la façon dont les étapes susmentionnées doivent être suivies. Ainsi, la création d'une procédure ou d'un plan officiel « d'intervention en cas d'incident » s'avère extrêmement utile pour indiquer la voie à suivre avant et après un incident de sécurité informatique.

Au cours de l'établissement de la procédure ou du plan, il est important de réfléchir à la manière dont l'informatique judiciaire s'intègre à chacune des étapes susmentionnées, et ce, de la détection d'un incident à l'analyse après l'incident. Par exemple, l'étape du « rétablissement du service », plus particulièrement, pourrait avoir des répercussions considérables sur une enquête criminelle si certaines précautions ne sont pas prises. Afin de tenir compte de l'informatique judiciaire pendant l'établissement ou la révision d'un plan d'intervention en cas d'incident, il est important de bien comprendre ce que l'on entend par « informatique judiciaire ».

Le terme « informatique judiciaire » désigne la conservation, la détermination, l'extraction, la documentation et l'interprétation de données informatiques¹. Aux fins de la recherche de documents sur le sujet, plusieurs autres termes peuvent être considérés comme des synonymes, tels que « données judiciaires », « expertise informatico-judiciaire » et « expertise judiciaire numérique ». Cependant, certains diront que les différents termes peuvent sous-entendre un secteur d'analyse plus précis ou plus spécialisé.

[TRADUCTION]

L'informatique judiciaire constitue désormais un ensemble établi de disciplines, et les normes très strictes instaurées pour conserver les éléments provenant des ordinateurs personnels créent de fortes attentes relativement aux autres formes de preuves numériques, y compris celles qui sont recueillies dans les systèmes et les réseaux intégrés importants, dans Internet ainsi que dans les nouvelles séries d'assistants numériques personnels (ANP), de téléphones cellulaires et de lecteurs multimédias portatifs².

Pour les besoins du présent document, nous préférons utiliser la citation ci-dessus afin de définir de façon générale l'expression « informatique judiciaire », vu qu'elle laisse entendre que divers systèmes, appareils ou réseaux font partie des sources possibles aux fins de la collecte d'éléments de preuve et de l'analyse judiciaire.

1.1 Objectif

Le présent document a pour objectif de fournir aux premiers intervenants, comme le personnel de la sécurité des TI ou le personnel administratif, un guide technique en ce qui concerne l'informatique judiciaire ainsi que l'intervention en cas d'incident de sécurité informatique. Les ministères et organismes fédéraux peuvent utiliser ce guide pour élaborer ou pour mettre à jour leurs procédures ou leurs plans d'intervention en cas d'incident de sécurité informatique. Des procédures, des plans ou des documents à jour en matière d'intervention en cas d'incident peuvent jouer un rôle important lorsque le personnel de la sécurité des TI doit confier aux responsables de l'application de la loi des enquêtes sur des incidents qui semblent être de nature « criminelle » sans compromettre ou endommager les preuves numériques. Ce guide aide à clarifier la définition des délits informatiques, donne un aperçu de la participation des organismes d'application de la loi et des aspects juridiques, recommande les meilleures pratiques concernant l'intervention en cas d'incident informatique, et fournit d'autres renseignements connexes.

Le présent document est de nature préliminaire. Il ne vise pas à traiter du sujet de façon détaillée et il sera mis à jour régulièrement, à mesure qu'évoluent les méthodes judiciaires et les meilleures pratiques.

1.2 Hypothèses

Politique du ministère sur la sécurité – Le présent document tient pour acquis que le ministère respecte la norme concernant la *Gestion de la sécurité des technologies de l'information (GSTI)* du Secrétariat du Conseil du Trésor (SCT), et qu'il a établi une politique ministérielle sur la sécurité. La politique doit renfermer des renseignements précis sur des sujets tels que la surveillance de l'utilisation du réseau, l'utilisation acceptable des ressources informatiques et les politiques de vérification.

Politique du ministère sur l'intervention en cas d'incident – Le présent document tient également pour acquis que le ministère a établi un lien avec le Centre canadien de réponse aux incidents cybernétiques (CCRIC) de Sécurité publique Canada, et qu'il a élaboré un plan d'intervention en cas d'incident. Il s'agit d'une politique ou d'un plan à mettre en œuvre en cas d'incident de sécurité informatique.

2 Aperçu du problème

Désormais, les délits informatiques font régulièrement les manchettes de l'actualité. Aussi communs ces incidents soient-ils, il est probable que les violations des politiques d'utilisation acceptable (PUA) des ministères soient encore plus fréquentes. Bien que l'on puisse supposer que les crimes constituent toujours des violations de la PUA d'un ministère, une violation de la politique ministérielle sur la sécurité n'est pas toujours un crime. C'est là que réside le problème.

Que se passe-t-il lorsqu'un incident est décelé et que l'on ne sait pas au juste si une loi a été violée? L'informatique judiciaire est une tâche qu'il vaut mieux laisser aux professionnels dûment qualifiés, surtout lorsqu'il est possible que les éléments de preuve découverts au cours de l'enquête soient présentés devant les tribunaux. En même temps, les organismes d'application de la loi doivent souvent composer avec une charge de travail déjà lourde et ne peuvent être appelés à enquêter sur chaque incident pouvant constituer un crime. La façon de gérer ces situations difficiles est abordée dans le présent document, lequel traite aussi des meilleures pratiques qu'un ministère ou un organisme peut mettre en œuvre pour s'assurer que l'enquête préliminaire visant un incident de sécurité informatique se déroule sans heurts.

3 Meilleures pratiques

3.1 Règlement d'un incident et intervention

L'intervention en cas d'incident comprend la mise en œuvre de méthodes normalisées d'intervention en cas d'incidents de toute sorte. Dans le cas présent, le plan traitera expressément des incidents de sécurité informatique. Lors de tels incidents, il est important de s'attendre au pire puis de déclasser la situation. Conformément à la Norme opérationnelle de sécurité concernant la GSTI, les ministères doivent avoir un coordonnateur de la sécurité des TI, chargé de gérer les incidents de sécurité de l'information et de les signaler aux cadres supérieurs³. Tous les ministères fédéraux doivent également établir un plan d'intervention en cas d'incident. Les personnes chargées d'intervenir doivent prendre des notes détaillées sur les mesures prises pour déceler un incident, pour atténuer les dommages et pour mener une enquête⁴.

L'une des principales raisons pour lesquelles il faut prendre des notes si détaillées est que de nombreux incidents qui sont réellement graves débutent souvent par une anomalie inoffensive dans le système. Un petit pépin peut s'avérer n'être que la « partie émergée de l'iceberg ». Une violation apparente de la politique peut rapidement devenir un crime en soi. Ce qu'il faut retenir, c'est que dès qu'il est établi qu'un incident est un crime, il faut communiquer avec les organismes d'application de la loi. L'enquête interne doit alors cesser immédiatement, jusqu'à ce que des conseils soient obtenus auprès des autorités. Cette mesure vise à éviter de compromettre l'enquête ainsi que d'enfreindre la loi au cours de l'enquête.

3.2 Détection des incidents de sécurité informatique

A priori, l'un des principaux aspects de l'intervention en cas d'incident informatique est la façon dont l'incident est détecté. Sans la détection, il est impossible de savoir qu'une activité non autorisée a eu lieu sur le réseau. L'incident qui donne lieu à une enquête initiale peut être complètement inoffensif et être aussi simple qu'un rendement anormal du système ou du réseau. En fin de compte, il est important de considérer tout comportement anormal du système comme douteux, ce qui signifie qu'il faut preuve de circonspection au moment de recueillir des renseignements (éléments de preuve) sur le problème. Si le système est traité avec circonspection et qu'un crime est découvert, les lieux du crime risquent moins d'avoir été modifiés. Si l'incident est en fait anodin, l'enquêteur est plus à même de régler le problème et dispose de meilleures notes pour effectuer son travail.

Cependant, afin de pouvoir détecter de telles anomalies, il faut connaître les paramètres d'exploitation normaux. Pour ce faire, le personnel chargé de la TI doit effectuer des travaux de préparation avant qu'un incident de sécurité informatique ne survienne. Il est nécessaire de documenter le comportement des systèmes, des appareils, des systèmes d'exploitation et des réseaux qui sont utilisés chaque jour. En plus de détecter les incidents de sécurité informatique, cela permet également au personnel de déterminer s'il existe d'autres problèmes. La création de tels seuils peut se faire de plusieurs façons, dans plusieurs secteurs, notamment de la manière suivante :

- établir des installations de base pour chaque groupe de systèmes;
 - documenter les correctifs installés pour le système d'exploitation, les logiciels tiers installés et si ceux-ci ont reçu le correctif nécessaire, de même que toute configuration spéciale du système;
- connaître le rendement du système (connaître le type de rendement normal ou anormal);
- connaître l'utilisation du système (connaître le type de charge normal ou anormal).

Les autres méthodes de détection des incidents et des attaques comprennent les appels de la part d'utilisateurs attentifs au service de dépannage. Les utilisateurs sont souvent parmi les premières personnes à remarquer qu'un système ne fonctionne plus comme il se doit ou affiche un comportement anormal. La GSTI (article 14.2) souligne qu'il est important que les ministères offrent, au personnel de

leur service de dépannage, une formation sur la façon d'intervenir en cas d'incident de sécurité⁵. Lorsque des utilisateurs appellent et fournissent des renseignements sur un incident, le service de dépannage doit disposer d'une procédure d'intervention écrite indiquant le personnel de la sécurité des TI à contacter ainsi que les instructions à fournir à l'appelant.

Une autre méthode très commune pour la détection des incidents de sécurité informatique consiste à recourir aux technologies qui surveillent les systèmes et les réseaux afin de déceler les atteintes à la sécurité. Les outils de détection créent des alertes, comme des fichiers journaux, des courriels et d'autres types d'avis visant à attirer l'attention sur quelque chose qui pourrait être problématique. Il existe de nombreux types d'appareils et d'applications qui peuvent exercer de telles fonctions, notamment les suivants :

- les pare-feux (fichiers journaux);
- les routeurs (fichiers journaux);
- les systèmes de détection d'intrusion basés sur l'hôte;
- les systèmes de détection d'intrusion basés sur le réseau;
- les programmes d'adressage calculé des fichiers (programmes qui calculent à l'avance les condensés numériques pour les fichiers informatiques essentiels et qui permettent de valider les condensés numériques à la suite d'un incident).

L'article 17 de la norme concernant la GSTI expose qu'au minimum, les ministères doivent avoir une fonction de journal de vérification dans tous leurs systèmes de TI⁶. Les systèmes à risque élevé doivent être mieux protégés, ce qui comprend la mise en œuvre d'applications ou de dispositifs de détection des incidents automatisés et en temps réel. La mise en œuvre de ces différents moyens de défense est toutefois assujettie aux lois et aux politiques qui s'appliquent.

3.3 Participation des organismes d'application de la loi

La participation des organismes d'application de la loi à une enquête visant un incident de sécurité informatique peut être complexe. C'est pourquoi on préfère parfois ne pas faire appel à la police. Depuis longtemps, dans le cadre de l'intervention initiale en cas d'atteinte à la sécurité, il peut arriver que l'affaire ne soit pas signalée à la police. Cependant, il convient de noter que les organismes d'application de la loi peuvent offrir de nombreux avantages, tels que les suivants :

- fournir des données techniques, des profils de pirates informatiques, des signatures de dossier et des valeurs d'adressage calculé;
- offrir des avis juridiques pour une affaire pénale;
- fournir des lignes directrices et des meilleures pratiques en matière de sécurité des TI;
- coordonner la collaboration du fournisseur d'accès Internet (FAI);
- élaborer une activité opérationnelle ciblée (fondée sur un nombre élevé d'incidents signalés);
- trouver un suspect;
- mener une analyse statistique des tendances, des points vulnérables et des méthodes criminelles à l'origine de l'élaboration de mesures de prévention nouvelles ou améliorées.

Selon la *Politique du gouvernement sur la sécurité* (PGS) du Secrétariat du Conseil du Trésor, dès qu'il est établi qu'un incident est un crime, l'organisme d'application de la loi compétent doit être appelé⁷. Selon le type de menace ou d'incident (p. ex. une menace à la sécurité nationale), il est possible que d'autres organismes doivent être informés, tels que le Service canadien du renseignement de sécurité (SCRS) et Sécurité publique Canada⁸.

3.3.1 Mesures qui précèdent l'application de la loi

Dans la plupart des cas, une enquête sur un incident de sécurité informatique débute avec le personnel technique sur place. Il s'agit de la première étape logique, puisque ce personnel est responsable des systèmes et de la sécurité de ceux-ci. Comme il serait très difficile, voire impossible, pour les responsables de l'application de la loi d'intervenir dans chaque incident détecté (qui n'est pas encore considéré comme un « crime »), on peut s'attendre à ce que le personnel technique soit appelé à prendre certaines mesures d'enquête.

Il est important d'enquêter sur le système suspect uniquement dans la mesure strictement nécessaire afin de déterminer si la participation des services de police est requise. Cela est particulièrement vrai s'il est déjà évident que le problème est lié à la sécurité. Le personnel qui procède à l'examen initial doit noter tout ce qu'il fait et touche. Toutes les pages de notes doivent être signées et datées. Ces notes se révéleront d'une très grande valeur si jamais l'incident donne lieu à une enquête criminelle.

Les mesures prises au cours de la phase initiale de l'enquête varient toujours selon la situation et le type de système analysé. Malheureusement, il est impossible de tenir une liste exhaustive des choses à faire et à ne pas faire, car la liste changerait constamment pour tenir compte des technologies et des méthodologies en pleine évolution.

Le meilleur moyen de comprendre les méthodes et les principes fondamentaux de l'informatique judiciaire est de suivre des cours de formation pratique sur le sujet. Les cours et les colloques en question se donnent partout au Canada et aux États-Unis. Ils visent à offrir une formation de base ou avancée, à faire comprendre les concepts judiciaires et juridiques importants, et à assurer une expérience concrète de l'analyse de systèmes types.

Étant donné que beaucoup de fournisseurs de formation judiciaire sont basés aux États-Unis, il ne faut pas oublier que, bien que les éléments de base des ordinateurs et leurs fonctions demeurent les mêmes, les différences entre les lois canadiennes et les lois américaines peuvent être importantes. Dans certains cas, un crime reconnu dans un pays n'est pas un crime dans l'autre pays.

Ces cours de formation portent également sur le recours à divers outils judiciaires qui peuvent être utilisés pour analyser un système suspect. Aujourd'hui, de nombreuses entreprises offrent des trousseaux à outils judiciaires pour la tenue d'enquêtes et la collecte d'éléments de preuve à présenter devant les tribunaux. Il existe également de nombreux programmes d'exploitation libre.

Le point à retenir au moment de sélectionner une trousse à outils est la crédibilité que celle-ci dégage devant les tribunaux. Les deux trousseaux à outils les plus couramment utilisés par les enquêteurs sont EnCase, de Guidance Software, et le Forensic ToolKit (FTK), de AccessData. Les deux trousseaux sont jugés acceptables dans les salles d'audience du Canada et des États-Unis. De plus, les deux entreprises offrent leur propre formation et leur propre certification afin de garantir l'utilisation adéquate des trousseaux.

À l'heure actuelle, les délits informatiques tiennent les responsables de l'application de la loi très occupés. Une fois qu'un incident est considéré comme un crime et que le ministère ou organisme a signalé l'incident, il est possible que les responsables de l'application de la loi ne soient pas en mesure d'intervenir immédiatement sur les lieux. Si des données essentielles risquent d'être perdues ou compromises avant l'arrivée des responsables de l'application de la loi, le ministère ou organisme peut devoir prendre des mesures préventives sur-le-champ. Un exemple de ce genre de situation serait la nécessité d'extraire des données volatiles d'un système suspect avant toute modification ou destruction.

- Données volatiles : Données qui seront perdues ou modifiées dans un bref délai ou dès la perte d'alimentation du système (hors tension); par exemple, la mémoire d'un système informatique (RAM système) ou des données opérationnelles soutenues par des routeurs.

Il est manifestement nécessaire d'extraire ce type de données de la mémoire avant que celle-ci ne soit modifiée ou perdue. La mémoire pourrait renfermer des preuves de mesures prises dans le système ou des renseignements sur les processus en mémoire au moment de l'incident. Si une situation survient où des données volatiles pourraient être perdues si elles ne sont pas extraites immédiatement, et que les agents de police ne sont pas en mesure d'intervenir immédiatement, le gestionnaire des systèmes ou le personnel de la sécurité technique doit extraire les renseignements afin de les conserver à des fins d'analyse par les organismes d'application de la loi.

Le personnel technique doit documenter, de façon précise et par écrit, tout ce qu'il fait. Ainsi, les données et les notes écrites pourront être présentées de manière efficace aux agents de police lorsqu'ils arriveront. Les services de police doivent parfois travailler avec la « meilleure preuve » qui peut être obtenue. Ce n'est peut-être pas l'idéal, mais il se peut qu'il s'agisse de la meilleure preuve disponible pour la situation en question. Enfin, il ne faut pas oublier que les services de police sont là pour aider. En cas de doute, il vaut mieux privilégier la prudence.

Le National Institute of Standards & Technology des États-Unis a rédigé un document exhaustif à l'intention du personnel chargé de la TI qui travaille à la première ligne d'intervention en cas d'incident informatique. Pour obtenir de plus amples renseignements et des documents, veuillez consulter le guide du National Institute of Standards & Technology, intitulé *First Responders Guide to Computer Forensics: Advanced Topics*⁹.

3.3.2 Communication avec les organismes d'application de la loi

La décision de communiquer avec les organismes d'application de la loi doit être prise selon le cas. Tous les incidents sont différents, et la nécessité d'une intervention policière peut devenir évidente à divers moments au cours de l'enquête.

Dans certains cas, il est difficile de faire la distinction entre des incidents considérés comme « criminels » et des violations de la politique du ministère sur la sécurité. Il est parfois évident qu'un crime a été ou est commis. Dans d'autres cas, ce n'est pas aussi évident, et un professionnel qui connaît le *Code criminel* doit être consulté. Les ministères fédéraux qui font face à un incident de sécurité informatique nécessitant l'intervention de la police doivent communiquer avec le groupe intégré de la criminalité technologique (GICT) compétent de la GRC. Ces groupes sont situés dans les villes centres du Canada. Toute activité ou incident criminel présumé découvert par tout autre organisme doit être signalé au service de police local.

Au moment de communiquer avec la police, il faut être prêt à fournir des précisions sur l'activité ou l'incident criminel présumé. Si tous les faits sont à portée de la main, il sera plus facile de déterminer si l'intervention de la police est nécessaire. Si la police se rend sur les lieux, il faut être prêt à lui fournir des renseignements.

La police devra consulter toutes les notes prises. Il convient de noter que la police peut devoir saisir les documents originaux comme éléments de preuve; par conséquent, il est bien de photocopier les documents avant de les remettre. Des fichiers journaux du système peuvent également être demandés. Si certaines dates ou heures indiquées dans un fichier journal jouent un rôle important relativement à l'incident, il peut être utile d'imprimer le fichier. Dans la mesure du possible, il faut surligner les éléments préoccupants afin qu'il soit plus facile de les repérer. Les renseignements fournis aux agents de police

lorsque ceux-ci se rendent pour la première fois sur les lieux peuvent déterminer l'orientation et la portée de l'enquête. Soyez prêts!

3.4 Aspects juridiques

Pour les besoins du présent document, le terme « délits informatiques » désigne des actes criminels qui comprennent l'utilisation d'un ordinateur ou d'un réseau. Toutefois, en matière d'informatique judiciaire, des preuves numériques peuvent également être utilisées afin d'appuyer les poursuites intentées contre les auteurs d'autres actes criminels. Les articles suivants du *Code criminel* du Canada définissent les actes relatifs aux ordinateurs, aux réseaux et aux données qui sont considérés comme criminels au Canada.

- Article 326 – Vol de service de télécommunication
- Article 342.1 – Utilisation non autorisée d'ordinateur
- Article 342.2 – Possession de moyens permettant d'utiliser un service d'ordinateur
- Article 430(1.1) – Méfait concernant des données

3.4.1 Preuve¹⁰

Dans le cadre des enquêtes relatives à l'informatique judiciaire et aux délits informatiques, le terme « preuve » désigne « tout renseignement lié à un incident d'une forme physique ou binaire (numérique) pouvant être utilisé afin d'appuyer ou de prouver les faits d'un incident ». Le concept de la « meilleure preuve » se rapporte à la preuve qui correspond le mieux à la preuve originale ou tangible. Il peut s'agir du support original ou de la meilleure copie possible des données du point de vue judiciaire (copie du train de bits).

Parfois, les organismes d'application de la loi doivent se contenter de la « meilleure preuve », ce qui est souvent le cas lorsqu'une enquête initiale est confiée à la police. La police doit aussi examiner la meilleure preuve si une saisie du système informatique opérationnel a été effectuée parce qu'elle ne pouvait se rendre sur les lieux assez rapidement. Par conséquent, il est important de comprendre les exigences de la police en ce qui concerne les enquêtes préliminaires et la manipulation de la preuve, afin d'être en mesure d'offrir aux agents la meilleure preuve possible.

3.4.2 Règles de preuve¹¹

Les règles de preuve sont très précises et visent à garantir que la preuve est obtenue et stockée comme il se doit et qu'elle n'a pas été modifiée lorsqu'elle est présentée devant les tribunaux. Selon les règles, les preuves numériques doivent être :

- **authentiques** – l'intégrité et la chaîne de possession des éléments de preuve doivent être intactes;
- **complètes** – tous les éléments de preuve qui appuient ou qui contredisent toute preuve qui inculpe un suspect doivent être étudiés et évalués. Il est également nécessaire de réunir des éléments de preuve qui permettent d'éliminer d'autres suspects. On ne doit pas seulement être capable de prouver que l'accusé a commis le crime, mais on doit également prouver que le crime n'a pas été commis par quelqu'un d'autre;
- **fiables** – les procédures et les outils relatifs à la collecte, à l'examen, à l'analyse et à la conservation des preuves ainsi qu'à l'établissement de rapports s'y rattachant doivent permettre d'arriver aux mêmes résultats au fil du temps. Les procédures ne doivent pas mettre en doute l'authenticité de la preuve et les conclusions tirées à la suite de l'analyse;
- **crédibles** – les preuves doivent être claires, faciles à comprendre et crédibles. La version des preuves présentées devant les tribunaux doit être liée à la preuve binaire originale, sans quoi il est impossible de savoir si la preuve a été contrefaite.

Il est tout aussi important de suivre les règles de preuve dans le cadre des enquêtes relatives à l'informatique judiciaire à caractère non pénal pour les deux raisons qui suivent. D'abord, les enquêtes à caractère non pénal peuvent également se rendre devant les tribunaux. Par exemple, les violations de la politique du ministère sur la sécurité peuvent entraîner la destitution d'un employé, et cet employé peut, par la suite, intenter une poursuite contre le ministère pour congédiement injustifié. La preuve devient essentielle pour faire en sorte que la destitution résiste à l'audience¹². Il est également important de disposer d'une politique qui puisse appuyer la décision de la destitution. Il s'agit d'un document que le ministère peut utiliser comme preuve que l'employé était au courant qu'il contrevenait aux règles.

Ensuite, une enquête préliminaire peut permettre de découvrir une activité criminelle. Une fois l'incident considéré comme criminel, tous les efforts déployés jusque-là doivent respecter les normes juridiques canadiennes afin de garantir que la preuve est admissible et que l'enquête n'a pas été compromise.

En mars 2000, le Groupe des Huit (G8) a établi un ensemble de principes proposés pour les procédures relatives à la preuve numérique. Ces principes offrent une base solide sur laquelle faire fond pendant tout examen effectué avant que les responsables de l'application de la loi n'interviennent.

- Principes du G8 – Procédures relatives à la preuve numérique¹³
 - Dans le traitement des preuves numériques, tous les principes judiciaires généraux et relatifs aux procédures doivent être appliqués.
 - Dès la saisie de preuves numériques, les mesures prises ne doivent pas venir modifier ces preuves.
 - Lorsqu'il est nécessaire qu'une personne accède aux preuves numériques originales, cette personne doit avoir suivi une formation à cet égard.
 - Toutes les activités liées à la saisie, au stockage ou au transfert des preuves numériques ou à l'accès à ces preuves doivent être entièrement documentées, conservées et disponibles aux fins d'examen.
 - Une personne est responsable de toutes les mesures prises en ce qui a trait aux preuves numériques pendant que celles-ci sont en sa possession.
 - Tout organisme responsable de la saisie, du stockage ou du transfert des preuves numériques ou de l'accès à celles-ci est responsable de la conformité à ces principes.

Cet ensemble de principes peut servir de base solide. Cependant, tel qu'il est exposé dans l'un des principes, si une personne doit toucher aux éléments de preuve, elle doit avoir suivi la formation adéquate. La formation permet de réduire la probabilité d'une modification non intentionnelle de la preuve. Elle permet également de rehausser la crédibilité d'une personne devant la cour si elle est appelée à témoigner sur les mesures prises avant l'arrivée ou l'intervention des agents de police.

3.4.3 Chaîne de possession¹⁴

La chaîne de possession désigne le suivi des éléments de preuve recueillis sur les lieux du crime jusqu'à la présentation de ceux-ci devant les tribunaux. L'entretien de la chaîne de possession est essentiel dans les cas qui reposent fortement sur des preuves numériques. Ce type de preuve peut facilement être modifié, et un bris dans la chaîne de possession peut compromettre la force probante d'une affaire pénale. Il est essentiel de savoir où se sont trouvées les preuves en tout temps, du moment où elles ont été obtenues au moment où elles sont présentées devant les tribunaux¹⁵. Les organismes d'application de la loi préfèrent toujours qu'on ne touche pas à la preuve avant leur arrivée sur les lieux. Cependant, cela n'est pas toujours possible, tel qu'il a été mentionné précédemment. Dans de tels cas, toutes les mesures prises par le personnel ne faisant pas partie des organismes d'application de la loi doivent entretenir la chaîne de possession et respecter les règles de preuve.

4 Conclusion

Les enquêtes liées à la sécurité sont des situations complexes qui nécessitent de la patience, une expertise technique et une connaissance du droit. Il s'agit du type de problèmes qui devraient être gérés par une personne qui a une expérience du domaine. Cela est particulièrement vrai si l'on croit que l'incident est un crime. Le personnel technique qui est chargé d'intervenir en cas d'incident dans son ministère ou organisme devrait suivre une formation sur l'informatique judiciaire. Cela garantira un certain niveau fondamental de compétence dans le cas d'un examen initial. Cette formation permettra également de réduire la probabilité que des erreurs de principe soient commises pendant une analyse du système en question.

De préférence à la suite de directives données par un policier expert, le personnel technique peut saisir les données ou les renseignements d'un système suspect, si la politique du ministère sur la sécurité l'a déjà autorisé et qu'il a été déterminé que la mesure est opportune. Cela ne doit être effectué que si c'est une stricte nécessité. Toutes les mesures prises doivent être notées de façon détaillée, et les notes doivent être signées et datées. Des copies de ces notes doivent être remises aux agents de police qui se rendront sur les lieux plus tard.

Si un crime est présumé ou confirmé, la meilleure approche consiste à laisser le système et à communiquer avec l'organisme d'application de la loi compétent. Les agents donneront une orientation sur les subtilités de la criminalistique et du droit pénal canadien.

Les méthodes et les technologies judiciaires changent constamment, ce qui fait de ce domaine déjà complexe, un domaine dans lequel il est difficile de rester à jour. Cependant, grâce aux cours reconnus sur le domaine, et si l'on est toujours prêt à demander la participation d'experts en droit et en informatique judiciaire dans le cadre d'une enquête, il y a plus de chances que celle-ci se déroule sans heurts et donne un résultat favorable pour les personnes visées.

La GRC continuera de mettre le présent document à jour, à mesure que les meilleures pratiques, les outils et les méthodes évolueront.

¹ Warren G. Kruse et Jay G. Heiser, *What Exactly is Computer Forensics?*, juin 2004, p. 1, en ligne : IT Observer <http://www.ebcvg.com/articles.php?id=220>.

² Peter Sommer, *Directors and Corporate Advisors' Guide to Digital Investigations and Evidence*, septembre 2005, p. 9. Information Assurance Advisory Council, en ligne : <<http://www.iaac.org.uk/Default.aspx?tabid=65>>.

³ Secrétariat du Conseil du Trésor, *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information*, le 14 avril 2004, p. 3. Secrétariat du Conseil du Trésor, en ligne : <http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/23RECON_f.asp>.

⁴ *Ibid.*, p. 15.

⁵ GSTI, art. 14.2.

⁶ *Ibid.*, art. 17.

⁷ Secrétariat du Conseil du Trésor, *Politique sur la Sécurité*, le 1^{er} février 2002, p. 11. Secrétariat du Conseil du Trésor, en ligne : <http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/gsp-psg_f.asp>.

⁸ *Ibid.*, p. 11.

⁹ Le document du National Institute of Standards and Technology se trouve à l'adresse suivante : <http://www.cert.org/archive/pdf/05hb003.pdf>.

¹⁰ Centre de la sécurité des télécommunications, *Protection de l'infrastructure de l'information du gouvernement du Canada : Expertise judiciaire en informatique – Concept d'opération*, Ottawa : Cinnabar Networks Inc., 2004, p. 17.

¹¹ *Ibid.*, p. 18.

¹² National Infrastructure Security Coordination Center, « An Introduction to Forensic Readiness Planning », mai 2005, p. 3. NISCC, en ligne : <<http://www.niscc.gov.uk/niscc/docs/re-20050621-00503.pdf>>.

¹³ International Organization on Computer Evidence, « G8 Proposed Principles for the Procedures Relating to Digital Evidence », mars 1998, p. 1. National Center for Forensic Science, en ligne : <<http://ncfs.org/documents/ioce2002/reports/g8ProposedPrinciples.pdf>>.

¹⁴ Précité, note 5, p. 18.

¹⁵ Précité, note 1, p. 26 et 27.