Assurances

Assurances

Pour une meilleure défensive contre la fraude informatique

Yves Giard

Volume 52, numéro 2, 1984

URI : https://id.erudit.org/iderudit/1104376ar
DOI : https://doi.org/10.7202/1104376ar

Aller au sommaire du numéro

Éditeur(s)

HEC Montréal

ISSN

0004-6027 (imprimé)
2817-3465 (numérique)

Découvrir la revue

Citer ce document

Giard, Y. (1984). Pour une meilleure défensive contre la fraude informatique. *Assurances*, *52*(2), 160–167. https://doi.org/10.7202/1104376ar

Résumé de l'article

It is still difficult to say exactly what measures should be taken to prevent computer theft. Mr. Yves Giard's article indicates that a complete solution is very far away. Much more research on computer information will be needed, and solutions will probably emerge gradually, as we become more familiar with computer operations. For the moment, we can only discuss general ideas, and trust to luck, rather than science, to prevent theft or information leaks, or at least to detect them when they reach a certain scale. Currently, we have the impression of being, if not totally disarmed, at least with very little power of control over the numerous problems that can arise in the field of computer security. The author gives some ideas of accounting practices which are used in certain cases.

Pour une meilleure défensive contre la fraude informatique

par

Yves Giard, B.A.A., C.A.[1]

It is still difficult to say exactly what measures should be taken to prevent computer theft. Mr. Yves Giard's article indicates that a complete solution is very far away. Much more research on computer information will be needed, and solutions will probably emerge gradually, as we become more familiar with computer operations. For the moment, we can only discuss general ideas, and trust to luck, rather than science, to prevent theft or information leaks, or at least to detect them when they reach a certain scale.

Currently, we have the impression of being, if not totally disarmed, at least with very little power of control over the numerous problems that can arise in the field of computer security. The author gives some ideas of accounting practices which are used in certain cases.

~

Depuis l'avènement des micro-ordinateurs et l'élargissement considérable des applications de l'informatique, on a une meilleure compréhension de cet instrument de travail très répandu. Malheureusement, certains ont exploité la vulnérabilité de l'informatique et sa puissance à des fins malheureuses.

On retrouve des exemples de fraudes dans plusieurs sociétés commerciales et particulièrement dans les institutions financières, c'est-à-dire là où l'ordinateur est le principal dépositaire des actifs de l'entreprise. Le département du commerce américain estime que

---

(1) M. Giard est chef d'équipe, membre de la section vérification informatique et échantillonnage statistique appliqué à la vérification chez Caron, Bélanger, Dallaire, Gagnon & Associés, Clarkson Gordon.

pour une fraude informatique divulguée, il y en a cent qui ne le sont pas[2]. Bien que les institutions financières semblent les plus vulnérables, toute entreprise dont les actifs sont gérés à l'aide de l'ordinateur est susceptible d'être touchée. On peut imaginer facilement les répercussions qu'aurait la destruction des systèmes produisant les chèques de l'assurance-chômage ou des rentes, de même que les données accumulées dans le cadre de la recherche médicale ou dans le domaine spatial ou scientifique.

La difficulté que représentent les poursuites en ce domaine résulte de l'absence d'un environnement légal approprié. Jusqu'à récemment, les rapports informatiques ne constituaient pas un élément de preuve, dû à la difficulté que représente l'authentification de ces documents. De plus, les tribunaux ne sont pas encore bien préparés à traiter de ce type d'offenses. Enfin, les compagnies subissant des pertes reliées à l'informatique ne sont pas prêtes à subir les effets négatifs d'une telle publicité. En effet, il ne s'agit souvent pas de crimes contre la personne, mais bien de crimes contre un organisme. C'est d'ailleurs pour cela que le public en général est plus indulgent vis-à-vis ce genre de situation que si des individus sont lésés. De plus, étant donné la complication des ordinateurs, on associe souvent aux personnes ayant effectué des actes frauduleux une intelligence ou, tout au moins, une débrouillardise exceptionnelle.

Cette situation d'élitisme tend à favoriser le déploiement de ces actes plutôt qu'à les empêcher.

Plusieurs tendances se dessinent actuellement en matière informatique :

- une croissance sans précédent du matériel et des logiciels disponibles et utilisés en raison d'une baisse considérable de leur prix ;
- un grand raffinement des techniques d'intégration des systèmes d'information ;
- l'adoption généralisée de l'informatisation à tous les paliers de gestion.

~

(2) *Bureau of Justice Statistics*, U.S. Department of Justice, Washington, D.C.

Ces facteurs et l'utilisation prochaine des méthodes électroniques de transferts monétaires permettent de s'interroger sur les méthodes suivies par les directeurs de centres informatiques, pour essayer d'empêcher ou, tout au moins, de détecter les fraudes commises qui sont effectuées par le biais de l'ordinateur.

Bien qu'il ne s'agisse pas ici d'énoncer toutes les mesures de prévention, ni toutes les méthodes utilisées pour perpétrer des fraudes informatiques, quelques cas typiques permettront d'apprécier davantage la nature des méthodes utilisées.

Très différent du crime traditionnel, ce genre de fraude comprend la manipulation des données et des programmes, dont voici un aperçu.

Manipulation des données

C'est la façon la plus facile et, certainement, la plus utilisée des fraudes reliées à l'ordinateur. Elle implique la modification des données avant ou durant leur entrée à l'ordinateur. Le changement peut être fait par quiconque est associé aux procédés de création, d'enregistrement, d'examen ou de transformation des données devant résider en mémoire. On peut, par exemple, forger des documents, échanger des supports magnétiques valides pour d'autres préparés d'avance, et violer des données d'entrée ou leur contrôle.

Un exemple typique de ce genre de fraude concerne un commis responsable de l'entrée des données sur les heures de travail de trois cents employés. Il a noté que, bien que le nom et le numéro de l'employé soient entrés sur l'ordinateur, celui-ci n'utilise que le numéro de l'employé dans le traitement et l'impression des chèques. De plus, les procédés de contrôle manuel ne reposent que sur les noms d'employés, puisque personne n'identifie les gens par leur numéro. Il a su profiter de cette situation et a complété des formulaires de temps supplémentaire, portant le nom de certains employés et son propre code personnel.

Un système de contrôle bien conçu permettrait d'associer quelques lettres du nom de l'employé et son numéro.

Manipulation des programmes

La manipulation des programmes consiste à placer des instructions dans un programme, de telle sorte que l'ordinateur puisse effectuer des fonctions ou procédés non autorisés. L'exemple le plus souvent cité consiste à transférer l'agrandissement excédentaire des calculs d'intérêts à un compte unique, plutôt que de le répartir au fur et à mesure de sa création.

Plusieurs autres moyens existent pour commettre des fraudes par ordinateur, telles que le vol des données, programmes, rapports ou encore l'écoute électronique. Des moyens qui ne sont pas connus aujourd'hui feront sûrement l'objet de révélation par la presse écrite et électronique de demain.

Les résultats d'études entreprises aux États-Unis démontrent que la raison principale de l'inquiétude vis-à-vis la fraude informatique est sa difficulté de découverte, portant généralement sur une période de deux à trois ans, dans certains cas, de six ans.

Les raisons principales de cette situation sont les suivantes :

- la vitesse d'exécution des transactions frauduleuses qui peuvent être complétées dans une fraction de seconde ;
- le manque de piste de vérification lorsqu'il n'y a pas d'évidence de l'opération ;
- la localisation du fraudeur ; en effet, les réseaux de communication et les terminaux éliminent le besoin d'être présent physiquement au centre de traitement ;
- l'étendue des pertes : la fraude informatique dans le monde se situe à environ $300 millions par année.

La perte moyenne due à l'informatique inclut :

- pertes d'inventaire : moyenne de $1,3 million ;
- comptes de dépôt : moyenne de $500,000 ;
- comptes à payer : moyenne de $324,000 ;
- salaires : moyenne de $139,000.

Le *Federal Bureau of Investigation* estime aussi qu'une fraude par ordinateur au niveau bancaire se situe à environ $500,000, comparativement à une fraude manuelle de $23,500.

Le crime par ordinateur peut donc être une activité relativement lucrative et comporter peu de risques. En effet, un certain Jerry Schnyder aurait volé $1,2 million à la *Pacific Telephone.* Il fut condamné à dix-huit mois de prison, mais n'en aurait purgé que trois.

~

La dépendance de plus en plus grande des compagnies au besoin de continuité des opérations informatiques constitue un élément additionnel, justifiant la plus grande sensibilité accordée à la fraude ou l'utilisation malhonnête des systèmes informatiques. Les grandes compagnies de produits chimiques aux États-Unis estiment qu'une période de trente-six heures sans ordinateur amènerait la fermeture de la corporation. Les grands manufacturiers canadiens croient que, sans leur système d'entrée des commandes, ils ne sauraient plus quoi fabriquer après une période de neuf heures. Les grandes compagnies d'assurance-vie canadiennes estiment qu'il s'ensuivrait une dégradation très importante de leurs opérations après un délai de trois jours sans l'informatique. Tandis que les établissements bancaires considèrent qu'ils sont entièrement sous la dépendance de l'ordinateur.

Notre expérience démontre cependant que plusieurs clients ont établi des solutions de la sécurité informatique bien personnelles. Par exemple, un ministère qui avait des mesures sévères de sécurité, au niveau de l'accès à la salle des ordinateurs, n'avait à peu près aucun contrôle sur les 1,100 usagers des terminaux donnant accès au système informatique. D'autres exemples démontrent que beaucoup de compagnies qui ont pris des mesures sécuritaires pourraient facilement les améliorer.

~

Mais quel est le rôle du vérificateur externe dans ce domaine ? Comment ce rôle se compare-t-il à la vérification annuelle ? Tout d'abord, nous nous devons de mentionner que les objectifs sécuritaires sont bien différents de la vérification annuelle. En effet, le but d'une vérification comptable ordinaire est de faire rapport sur la fidélité de la présentation des états financiers annuels. Tandis que l'étude des mesures sécuritaires vise à évaluer la qualité des contrôles desti-

nés à protéger ou à minimiser la probabilité future des événements suivants :

- désastre naturel ;
- acte de violence ou de sabotage ;
- bris d'équipement (équipement informatique ou système de support tel que l'air climatisé et l'électricité) ;
- acte criminel (vol de rubans magnétiques, de disques, de programmes, de données, des accès non autorisés, divulgations).

D'autre part, l'approche d'une vérification diffère d'une revue de sécurité principalement par les éléments suivants. Lors d'une vérification, l'expert-comptable ne fait pas une revue détaillée de tous les systèmes, puisque certains n'ont pas une incidence directe sur les états financiers ou parce que des procédés alternatifs de vérification peuvent être effectués plus économiquement. D'autre part, l'objet de la vérification est de revoir et d'évaluer les contrôles internes, afin de déterminer l'étendue, la nature et le calendrier des procédés de vérification. L'objectif n'est pas de produire une opinion indépendante sur la qualité des contrôles internes.

Cependant, la revue de la sécurité veut revoir toutes les activités informatiques et seulement celles-ci. L'emphase primaire est sur la prévention et le recouvrement ; l'emphase secondaire est sur les mécanismes permettant de détecter les erreurs et les irrégularités.

Enfin, les risques d'une vérification financière font en sorte que plusieurs décisions vis-à-vis l'étendue de la révision sont définies à l'aide de critères prédéfinis d'importance relative. Cependant, lors d'une revue de sécurité, il n'y a pas vraiment de directives à cet égard. Tout risque doit être évalué en termes de la probabilité et des coûts inhérents à l'occurrence des événements pouvant porter atteinte à la sécurité.

Sommairement, la revue financière décrit ce qui s'est passé, alors qu'une revue de la sécurité évalue ce qui pourrait arriver.

Tenant compte de ces considérations, voyons comment le vérificateur, chargé de revoir la sécurité informatique plutôt que de donner une opinion sur les états financiers, entreprendrait son pro-

gramme de travail. Tout d'abord, le travail serait divisé en cinq grandes sections que voici :

- l'équipement informatique ;
- le fichier de secours et recouvrement ;
- le point d'entrée ;
- le profil de sécurité informatique ;
- le développement d'un programme continu d'assurance de la qualité.

166 Équipement informatique

Cette section concerne la revue des pratiques actuelles de sécurité informatique de façon approfondie. Ainsi, cette revue permet à la compagnie de déterminer les niveaux de sécurité où elle se situe ; elle constitue un point de départ pour entreprendre un programme approfondi de sécurité informatique. À titre d'exemple, ce secteur couvre la sécurité physique, les pratiques à l'égard du personnel, les communications et les terminaux à distance, les opérations, les équipements, le logiciel informatique de même que les données et les programmes d'application.

Fichier de secours et recouvrement

Ce secteur comprend la revue des données critiques et des fichiers et les procédés de recouvrement et de copie de secours pour ces fichiers spécifiques. De plus, une revue des plans documentés et les procédures pour assurer la continuité du traitement dans l'éventualité où l'ordinateur de la compagnie deviendrait inopérant pour une période prolongée, serait aussi effectuée.

Point d'entrée

Cette revue concerne les systèmes existants afin de détecter les sources possibles d'entrée des opérations non autorisées et comment elles pourraient être entrées sur le système, en envisageant les possibilités de fraude. Spécifiquement, cette revue inclut les secteurs suivants :

- déterminer si les gens peuvent mal utiliser leur autorisation pour introduire des opérations fictives ;
- déterminer si les opérations peuvent être manipulées après leur autorisation ;

– évaluer les méthodes utilisées pour détecter les opérations non autorisées.

Profil de sécurité informatique

Ce secteur comprend l'évaluation des normes en vigueur lors du développement des systèmes, afin de revoir les responsabilités et les critères d'autorisation permettant d'accéder et de mettre à jour les données de la compagnie. Cette méthodologie prévoit donc les mesures préventives, lors du développement du système plutôt que les mesures correctives postérieures.

Développement d'un programme continu d'assurance de la qualité

Ce secteur comprend le développement des directives et des procédures à mettre en place par la compagnie, afin d'assurer un déploiement continu de son secteur de la sécurité informatique. Normalement, ce secteur relève du service informatique.

Il va sans dire que ce programme de travail est très différent d'une vérification annuelle, et l'on se doit de reconnaître que l'objet n'est pas de donner une opinion sur les états financiers, mais bien d'évaluer la qualité des mesures préventives dont le client dispose ou que nous lui suggérons de se donner, afin d'assurer un contrôle suffisant sur les ressources informatiques dont dépend le succès de son entreprise et sa continuité.

Conclusion

Tels sont les éléments qui nous paraissent souhaitables, en vue d'une meilleure défense contre la fraude informatique. La fraude, notons-le à nouveau, est souvent très difficile à détecter par suite des divers aspects qu'elle prend et que, au premier abord, l'ordinateur peut difficilement indiquer. Et c'est pourquoi on ne saurait trop revenir sur les mesures sécuritaires que le vérificateur interne ou externe est en mesure de conseiller.