Document généré le 17 juil. 2024 08:27

Assurances

Assurances

La fraude informatique : une nouvelle forme de criminalité

Monique Dumont

Volume 49, numéro 3, 1981

Introduction à l'informatique

URI : https://id.erudit.org/iderudit/1104145ar
DOI : https://doi.org/10.7202/1104145ar

Aller au sommaire du numéro

Éditeur(s)

HEC Montréal

ISSN

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

Découvrir la revue

Citer ce document

Dumont, M. (1981). La fraude informatique : une nouvelle forme de criminalité. *Assurances*, *49*(3), 293–297. https://doi.org/10.7202/1104145ar

Résumé de l'article

The author cites various cases of fraud made possible by virtue of a thorough knowledge of the computer. In recent years, activities of this nature have been particularly recurrent in the U.S. and in the following article, Monique Dumont incites electronic data processing users to secure the broadest form of crime insurance possible so as to be covered in the event of a costly fraud.

Tous droits réservés © Université Laval, 1981

Ce document est protégé par la loi sur le droit d'auteur. L'utilisation des services d'Érudit (y compris la reproduction) est assujettie à sa politique d'utilisation que vous pouvez consulter en ligne.

https://apropos.erudit.org/fr/usagers/politique-dutilisation/

érudit

Cet article est diffusé et préservé par Érudit.

Érudit est un consortium interuniversitaire sans but lucratif composé de l'Université de Montréal, l'Université Laval et l'Université du Québec à Montréal. Il a pour mission la promotion et la valorisation de la recherche.

https://www.erudit.org/fr/

La fraude informatique: une nouvelle forme de criminalité

par

MONIQUE DUMONT

The author cites various cases of fraud made possible by virtue of a thorough knowledge of the computer. In recent years, activities of this nature have been particularly recurrent in the U.S. and in the following article, Monique Dumont incites electronic data processing users to secure the broadest form of crime insurance possible so as to be covered in the event of a costly fraud.

~

Introduction

Les statistiques que l'on possède quant aux fraudes informatiques ne constituent que la pointe de l'iceberg, d'autant plus que les institutions financières en sont les premières victimes et qu'elles ne déclarent pas ou peu cette criminalité particulière.

Selon un article récent publié dans B*usiness* W*eek* du 20 avril 1981 aux pages 86 à 92 et intitulé «*Information processing: the spreading danger of computer crime*», trois facteurs vont contribuer à une hausse de la criminalité reliée à l'utilisation de l'informatique. Ce sont:

— le coût de plus en plus bas des ordinateurs qui sont maintenant accessibles aux particuliers;

— l'augmentation du nombre d'étudiants et d'individus qui acquièrent les connaissances de base sur l'utilisation de l'informatique;

— l'utilisation accrue de l'informatique dans les entreprises en facilite l'accès, par l'usage du terminal, à un nombre croissant d'employés.

Dunn R. Parker, l'auteur de l'ouvrage bien connu «*Computer by crime*», évalue que les seules fraudes rapportées en une année équivalent à des pertes de plus de 100 millions en dollars U.S.

Il ajoute que l'habileté des fraudeurs croît plus vite que celle des spécialistes de la sécurité, au même rythme que l'innovation technologique dans ce domaine.

De plus, le crime est payant: des chercheurs ont calculé qu'un vol à main armée rapportait en moyenne $9,000.00, un détournement de fonds $19,000.00 tandis que la fraude informatique pourrait rapporter, en moyenne, $450,000. Mais n'exagère-t-on pas?

Vulnérabilité des systèmes informatiques

L'ordinateur donne, à ceux qui le côtoient, un faux sentiment de sécurité qui est souvent amplifié par une incompréhension de son fonctionnement. D'autre part, selon les études qui ont été faites, la vulnérabilité des systèmes augmente avec leur complexité.

L'Association de Genève publiait, en octobre 1979 (Cahier 13) une étude intitulée «Les risques de pertes indirectes induites par les systèmes informatiques». On y trouve des données fort pertinentes sur le crime informatique et des statistiques recueillies par les chercheurs du Stanford Research Institute.

Le système informatique est principalement vulnérable en cinq points:

— à l'entrée des données (manipulation des données);
— la programmation (fausses instructions et programme modifié);
— au niveau du centre de contrôle (vol des enregistrements);
— à la sortie des données (vol de l'information; vente à un concurrent; espionnage industriel);
— par le réseau de transmission (intervention sur le réseau en intervenant directement par l'écoute ou l'interception des données).

Certains secteurs administratifs sont d'autre part privilégiés par les fraudeurs; ce sont:

— le vol des programmes informatiques qui peut devenir fort prisé par un concurrent;

— le vol de temps informatique ou lorsque l'employé l'utilise à des fins personnelles. Une étude en 1980 évaluait à $20.00 la minute les pertes de cette nature; c'est 20 à 100 fois ce que coûte le vol d'une minute d'utilisation d'un photocopieur traditionnel;

— les comptes recevables et les comptes payables (création de compagnies fictives);

— l'addition d'employés fictifs;

— les opérations de l'entreprise (listes de clientèle, nouveaux produits enregistrés sur bandes magnétiques, études de planification ou statistiques essentielles pour le développement de l'entreprise);

— le sabotage des installations et des inventaires.

Quelques exemples illustreront l'habileté des fraudeurs

A. Cas de peu d'importance

— Aux États-Unis, une banque fédérale reçoit l'ordre de transférer $16,000.00 d'une banque d'un État à un autre pour un nommé Michael Charles. L'opération s'est effectuée par téléphone, Charles ayant fourni à l'ordinateur le numéro de code exact du jour. Ce dernier, de son vrai nom ***, plaidait coupable, quelques mois plus tard, à l'accusation d'avoir trafiqué le réseau d'information de la réserve fédérale;

— Un programmeur d'ordinateur de 19 ans, à l'emploi d'une banque, se retrouve endetté d'une somme de $4,100.00. Il ordonne à l'ordinateur de transférer $100.00 de 41 comptes différents à un nouveau compte ouvert par sa femme sous un nom d'emprunt.

B. Cas importants

—1973— États-Unis - Equity Funding - $27,25 millions. Création de polices d'assurance fictives vendues aux réassureurs;

—1979–1981— États-Unis - Wells Fargo - $21,3 millions en dollars U.S.

***: Retraits d'argent frauduleusement déposé dans un compte de dépôt qui lui appartenait. L'interception des sommes se faisait lors de la transmission des sommes d'une succursale à l'autre. Pour éviter que le déséquilibre des comptes soit signalé par

l'ordinateur, il avait créé des crédits fictifs. L'opération dura 2 ans;

—1980— États-Unis - Security Pacific - $10,3 millions. Ayant eu connaissance du code de transfert employé ce jour-là en espionnant un collègue, *** transfert cette somme par téléphone à un compte suisse. Avant que la fraude ne soit découverte par les responsables de la sécurité, il avait pris l'avion, retiré l'argent et l'avait converti en diamants. Il fut arrêté quelques mois plus tard.

296

Les fraudeurs et les programmes de prévention

La fraude informatique est l'une des manifestations d'un nouveau type de criminalité: celle des cols blancs.

Les cols blancs, ce sont des cadres supérieurs des entreprises, des spécialistes (programmeurs, analystes), du personnel technique ou de soutien qui ont accès au système.

Les programmes de prévention sont, d'autre part, trop souvent négligés et l'une des causes de cette lacune dans la sécurité des systèmes réside dans l'ignorance des directions supérieures des entreprises, selon l'article du *Business Week.* La sécurité des installations se résume en effet, trop souvent, à la sécurité physique des installations, tandis que l'accès au système est largement établi.

Un très bon article vient de paraître dans le périodique *Canadian Data Systems,* intitulé «Analyzing Computer Security Risk» (pages 67 à 71), juillet 1981. L'article décrit les étapes d'analyse du risque, de son contrôle et des coûts. De nombreux tableaux complètent l'exposé théorique. On lira avec intérêt également l'article de MM. Bismuth et Giard en page 230 de notre revue.

Les institutions financières: des cibles privilégiées

Les institutions financières sont des cibles privilégiées pour les spécialistes (et néophytes) de la fraude informatique.

L'introduction des transferts électroniques de fonds (EFT: Electronic fund transfer) va offrir des occasions intéressantes aux fraudeurs dont la technologie permet de se brancher directement sur les réseaux de transmission.

Les banques travaillent donc conjointement avec les organismes de contrôle et les manufacturiers d'équipements électroniques antifraudes pour mettre au point, par exemple, des systèmes d'encodage électronique à l'épreuve des fraudeurs.

Les programmes sont doublement vérifiés et une supervision de cet ordre aurait permis de repérer plus rapidement la fraude commise contre la société Wells Fargo. (Citée plus haut).

Un expert de la sécurité des systèmes informatiques le notait dans une récente entrevue: «plus les criminels raffinent leurs méthodes, plus les systèmes doivent faire appel à une technologie sophistiquée».

Il faut cependant conclure que l'impression d'invulnérabilité que l'on constatait au début de cet article demeure et qu'il faudra d'autres fraudes coûteuses et retentissantes pour sensibiliser davantage les milieux d'affaires, à cette forme nouvelle de criminalité.

Constitutional Restrictions on the Power of Government and Inflation Expectations. Frank M. Engle Lecture. Wharton School of Business and Finance. Philadelphia, U.S..

The American College est à Philadelphie un centre d'enseignement extrêmement intéressant, qui se préoccupe surtout des questions d'assurance-vie et autre que vie. Chaque année, il confie à des conférenciers connus l'étude de questions ayant trait soit à la politique, soit à l'économie des États-Unis. Cette fois, le premier travail a trait à la constitution américaine, car là également se posent des problèmes assez graves, même s'ils n'atteignent pas l'intensité de ceux que présente la constitution canadienne. Quant à l'inflation traitée par M. Lindly H. Clark Jr, il n'y a pas, entre les États-Unis et nous, aucune autre différence que l'importance des chiffres en jeu, tant nos deux économies sont liées l'une à l'autre.