Assurances

Assurances

Computer Crime and Insurance

Henry Klecan

Volume 51, numéro 3, 1983

URI : https://id.erudit.org/iderudit/1104332ar
DOI : https://doi.org/10.7202/1104332ar

Aller au sommaire du numéro

Éditeur(s)

HEC Montréal

ISSN

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

Découvrir la revue

Citer ce document

Klecan, H. (1983). Computer Crime and Insurance. *Assurances*, *51*(3), 368–382. https://doi.org/10.7202/1104332ar

Résumé de l'article

L'usage des ordinateurs pose de sérieux problèmes de contrôle. Des sommes considérables peuvent être en jeu et faire l'objet de vol pur et simple, de détournements, de pertes prenant des formes diverses : brouillage des données, usage illicite des secrets de fabrication ou de commercialisation. À ces risques nouveaux, l'assurance apporte certaines solutions. L'auteur étudie le cas de deux polices émises, l'une par Lloyd's et l'autre par Aetna Casualty and Surety. Les deux garanties ont trait aux affaires traitées par les banques et autres institutions financières. Elles se limitent au vol sous diverses formes et comportent certaines exclusions qu'il faut connaître.

Computer Crime and Insurance

by

HENRY KLECAN, Jr., LL.L.[1]

L'usage des ordinateurs pose de sérieux problèmes de contrôle. Des sommes considérables peuvent être en jeu et faire l'objet de vol pur et simple, de détournements, de pertes prenant des formes diverses : brouillage des données, usage illicite des secrets de fabrication ou de commercialisation. À ces risques nouveaux, l'assurance apporte certaines solutions. L'auteur étudie le cas de deux polices émises, l'une par Lloyd's et l'autre par Aetna Casualty and Surety. Les deux garanties ont trait aux affaires traitées par les banques et autres institutions financières. Elles se limitent au vol sous diverses formes et comportent certaines exclusions qu'il faut connaître.

~

I — Introduction

With the increased use of computers in our working and recreational milieux, computer fraud or, if you wish, computer crime, has become a necessary consequence of our evolving society.

Computer related crime has been defined as any illegal act for which knowledge of computer technology is essential. In a comprehensive study of computer related crime prepared by SRI International for the U.S. Department of Justice, this area of crime was classified as follows :

> « Computer-related crime is the same in name as other familiar types of crime, including fraud, larceny, embezzlement, theft, sabotage, espionage, vandalism, burglary, extortion, and conspiracy. However, relative to the occupations of perpetrators, environments, modi operandi, forms of assets lost, time scales and geography, many computer-related crimes differ significantly from traditional crimes. The nature of business, economic, and white-collar crimes is changing rapidly as computers pervade the activities and environments in which these

---

[1] Mr. Henry Klecan is Vice President, Financial Institutions Insurance, Gérard Parizeau, Ltd., member of the Sodarcan group.

crimes occur. Computers are therefore engendering a new kind of crime in which they play four roles as objects, subjects, instruments, and symbols for deception. Based on a study of *669 cases of computer-related crime over the past 20 years*, the incidence of computer-related crime is increasing rapidly. This reflects the proliferation of computers in all segments of business ; local, state, and federal government ; and in society in general. »

Computer crime is now becoming the leader in « white collar » crimes whose perpetrators are said to be highly motivated, bright and energetic individuals between 18 and 30 years of age. The perpetrator will have all the information he needs to master the system and the security of the system will not have dissuaded him but rather have encouraged him to try to beat the computer.

The first criminal case involving a computer occurred in 1966 when a 21 year old programmer put a patch in a program used to process bank cheques and to detect overdraft accounts. The patch caused the computer to ignore overdrafts on the programmer's account. The programmer's activities were undetected until there was a computer breakdown.

II — Illustrations

The frauds committed are usually the consequence of simple minded techniques and yet, despite their simplicity, most of them are only detected by accident or after the disappearance of the perpetrators. To illustrate :

1. « Data Diddling » is the most common related method used in computer related crime. It involves changing date before or during data input to computers. The changing can be done by anyone, including non-employees, associated with or having access to the processes of creating, recording, transporting, encoding, examining, checking, converting and transforming data that ultimately enter a computer. Examples are exchanging valid computer tapes, cards or disks with prepared replacements ; source entry violations, punching extra holes or plugging holes in cards ; and neutralizing or avoiding manual controls.

   A typical example is the case of a timekeeping clerk of a railroad company who filled out data forms of hours

worked by 300 employees. All data on the forms that were entered into the housekeeping and payroll system on the computer used only employee numbers for processing. The employee took advantage of the system by filling out forms for overtime hours worked and using names of employees who frequently worked overtime but entering his own employee number. The employee's income increased by several thousand dollars every year until by chance an auditor examining federal income tax forms noticed the unusually high annual income of the clerk. While this loss was caused by an employee, a similar type of loss could occur to a financial institution where any person having access to data input could enter his customer's account number.

2. The trojan horse method is the covert placement of computer instructions in a program so that the computer will perform unauthorized functions but usually will still allow the program to perform its intended purposes. A typical business application program can consist of over 100,000 computer instructions and data. The trojan horse can also be concealed among 5 or 6 million instructions in the operating system and commonly used utility programs where it waits for execution of the target application program, inserts extra instructions in it for a few milliseconds of execution time, and removes them with no remaining evidence. Even if it is discovered, it is difficult to determine who may have done it except to narrow the search to those programmers who have the necessary skills, knowledge, and access among employees, *former employees, contract programmers, consultants,* or *employees of the computer or software suppliers.*

3. An automated form of crime involving the theft of small amounts of assets from a large number of sources is identified as a salami technique. For example, in a banking system the demand deposit accounting system for checking accounts could be changed (using the trojan horse method) to randomly reduce a few hundred accounts by 10 cents or 15 cents by transferring the money to a favored account where it can be legitimately withdrawn through normal methods. No controls are violated because the money is not removed from the system of ac-

counts. Instead, a small fraction of it is merely rearranged. The success of the fraud is based on the idea that each checking account customer looses so little that it is of little consequence. Here again the loss can be caused by anyone including *non-employees* who have obtained at some time access to the financial institution's programs.

4. « Superzapping » derives its name from superzap, a macro/ utility program used as a system tool. A computer center that has a secure computer operating mode needs a "Break glass in case of emergency" computer program that will bypass all controls to modify or disclose any of the contents of the computer. Utility programs such as superzap are powerful and dangerous tools in the wrong hands. They are normally used only by systems programmers and computer operators who maintain computer operating systems. However, they are often placed in program libraries where they can be used by any programmer or operator who knows of their presence and how to use them.

A classic example of superzappling resulted in a $ 128,000 loss to a bank in New Jersey. The manager of computer operations was using a superzap program to make changes to account balances to correct errors. The manager discovered how easy it was to make changes without the usual controls of Journal Records, and he made changes transferring money to three friends' accounts. They engaged in the fraud until a customer found a shortage in his account.

5. In another case, unknown individuals made off with $ 2,000,000 by exploiting a flow in the cheque-clearing system of a bank. The scheme made use of the fact that certain information was magnetically encoded on cheques so that they could be processed by computers. Among the magnetically pre-encoded information was a number enabling cheques to be returned to the bank on which they were drawn (the bank routing symbol) and the customer's account number.

The perpetrators obtained cheques from an east coast bank and encoded them with the bank routing symbol of a west coast bank. They then deposited the cheques in

the East Coast Bank and its computer duly sent them on to the west coast for payment. After three days, the East Coast Bank automatically assumed that the cheques had cleared and permitted the perpetrators to withdraw the funds.

Meanwhile, the West Coast Bank's computer had rejected the cheques because they appeared to be drawn on a closed account. Manual processing of the rejected cheques led to the conclusion that they had been misrouted, since the East Coast Bank's name was printed on the cheques. The cheques continued to travel between the two banks until someone became suspicious – by that time, the perpetrators had disappeared.(2)

A study of a number of computer related bank frauds indicated that the losses averaged $ 1,090,000 or about 10 times the average loss from all types of embezzlement.(3) Since 1966, there have been over 669 cases of computer related crimes in the U.S. and the incidence of this type of crime is increasing rapidly with the number of installed computers proliferating more rapidly.

In response to this growing exposure, a number of insurers have introduced a computer fraud cover, that is either attached as a complement policy to the bankers blanket bond or as an extension of the bankers blanket bond.

Both Lloyd's of London and the Aetna Casualty Company of Canada have introduced a computer fraud coverage which is available to both domestic and foreign based banks in Canada.

III — Insurance

Lloyd's of London was the first insurance market to introduce the electronic and computer crime policy in the fall of 1981 and subsequently revised it in February 1983. This crime coverage was added as a complementary policy to the bankers blanket bond.

The initial policy wording attracted immediate scrutiny and criticism from bank risk managers and insurance brokers alike. Complaints were directed 1) – at the cumbersome 35 page applica-

---

(2) Laurence J. Ochs, Esq. *Bank Insurance, Insuring Against Computer Fraud*, p. 2.

(3) Porter. *Computer Raped by Telephone*. New York Times, September 8, 1974.

tion questionnaire ; 2) – at a policy that dit not cover a bank's liability when it acted as a service bureau or intermediary for other banks' fund transfer ; the necessity for a security audit of the bank's E.D.P. System ; manifest intent had to be established by the assured to cause the assured to sustain a loss *and* to obtain financial benefit ; 3) – at the coverage uncertainty when the assured was unable to identify the perpetrator as an employee or not an employee.

In February 1983, Lloyd's of London introduced a revised version of their policy – broader and more flexible. According to some experts, it is considered to be the most comprehensive insurance policy available today in the field of computer fraud insurance.

The new Lloyd's Policy consists of seven different clauses from which the buyer can choose to tailer his own coverage.

The first clause covers losses caused by the tampering of a financial institution's own electronic fund transfer or computer system, the service bureau's computer system or a customer communication system.

INSURING AGREEMENT 1, COMPUTER SYSTEMS

By reason of the Assured having transferred, paid or delivered any funds or property, established any credit, debited any account or given any value as the direct result of the fraudulent input of Electronic Data directly into :

(1) the Assured's Computer Systems ; or
(2) a Service Bureau's Computer System ; or
(3) an Electronic Funds Transfer System ; or
(4) a Customer Communication System

or the fraudulent modification or the fraudulent destruction of Electronic Data stored within or being run within any of the above systems or during electronic transmission through data communication lines to the Assured's Computer Systems or a Service Bureau's Computer System which fraudulent acts were committed by a person who intended to cause the Assured to sustain a loss or to obtain financial gain for himself or any other person.

The first Lloyd's Policy provided coverage under several general insuring agreements for the fraudulent input, fraudulent modi-

fication and fraudulent destruction of electronic data in the Assured's Computer System, automated teller machines, Service Bureau's Computer System, and Communication Systems by a person "with the manifest intent to cause the Assured to sustain such loss and to obtain financial benefit".

The new insuring agreement 1 consolidates these several insuring agreements into one agreement and does away with the requirement to prove intent to cause a loss and obtain a financial benefit. Consequently, a loss resulting from a malicious act would be covered without showing a financial gain. Notwithstanding this

reformalised insuring agreement, what appears not to be covered is where hardware is changed such as to cause the output to be changed which would not be considered a modification of data.[4]

The second and third clauses cover losses resulting from the actual program tampering, fraudulent modification or destruction of the computer program or electronic instructions.

INSURING AGREEMENT 2, ELECTRONIC COMPUTER INSTRUCTIONS

By reason of the Assured having transferred, paid or delivered any funds or property, established any credit, debited any account or given any value as the direct result of the fraudulent preparation or the fraudulent modification of Electronic Computer instructions which fraudulent acts were committed by a person who intended to cause the Assured to sustain a loss or to obtain financial gain for himself or any other person.

INSURING AGREEMENT 3, ELECTRONIC DATA AND MEDIA

A. By reason of the malicious destruction or attempt thereat of the Assured's Electronic Data by any person while such data are stored within the Assured's Computer Systems or a Service Bureau's Computer System.

B. By reason of Electronic Data Processing Media being lost, damaged or destroyed as the direct result of robbery, burglary, larceny, theft, misplacement or mysterious unexplainable disappearance while the Electronic

[4] Laurence J. Ochs. *Ibid.* p. 14.

Data Processing Media is lodged or deposited within offices or premises located anywhere, or in the custody of a person designated by the Assured to act as its messenger (or a person acting as messenger or custodian during an emergency arising from the incapacity of such designated messenger) while the Electronic Data Processing Media is in transit anywhere, such transit to begin immediately upon receipt of such Electronic Data Processing Media by said messenger and to end immediately upon delivery to the designated recipient or its agent, provided that the Assured is the owner of such Electronic Data Processing Media or is legally liable for such loss or damage.

Insuring agreement 2 extends the coverage to independent contractors, consultants, programmers and any non-employee who modifies a software program no matter the mode used in accessing the computer to change the programs. Although the broad application of this coverage is limited by exclusion 2(T) which excludes loss resulting from fraudulent features contained in electronic computer instructions developped for sale to or are sold to multiple customers at the time of their acquisition from a vendor or consultant.

The coverage in insuring agreement 3 (a) is limited to only restoration costs and not lost income whereas 3 (b) excludes service bureaus and only covers lost data and not computer time for restoring the lost data.

The fourth clause covers fraud of funds, property, the establishment of any credit, the debiting of any account or the gaining of value when the banks acts upon fraudulent instruction received from an electronic communication system (which should be scheduled), an automated clearing house or by telex, TWX or similar means of communication. Unlike insuring agreement 6, where the fraudulent instructions emanate from the Assured, clause 4 covers fraudulent instructions received by the Assured.

INSURING AGREEMENT 4, ELECTRONIC COMMUNICATIONS

By reason of the Assured having transferred, paid or delivered any funds or property, established any credit, debited any account or given any value on the faith of any electronic communications directed to the Assured which were transmitted

or appear to have been transmitted through.

(1) an Electronic Communication system, or
(2) an Automated Clearing House, or
(3) by telex, TWX or similar means of communication

directly into the Assured's Computer Systems or to the Assured's Communications Terminal and fraudulent purport to have been sent by a customer, Automated Clearing House or financial institution but which communications were either not sent by said customer, Automated Clearing House or financial institution or were fraudulently modified during physical transit of Electronic Data Processing Media to the Assured or during electronic transmission through data communication lines to the Assured's Computer Systems or to the Assured's Communications Terminal.

INSURING AGREEMENT 6, ELECTRONIC TRANSMISSIONS

By reason of a customer of the Assured, an Automated Clearing House or a financial institution having transferred, paid or delivered any funds or property, established any credit, debited any account or given any value on the faith of any electronic communications purporting to have been directed by the Assured to its customer, an Automated Clearing House or a financial institution authorizing or acknowledging the trans fer, payment, delivery or receipt of funds or property which communications were transmitted or appear to have been transmitted through

(1) an Electronic Communications System, or
(2) an Automated Clearing House, or
(3) by telex, TWX or similar means of communication

directly into a Computer System or a Communications Terminal of said customer, Automated Clearing House or financial institution and fraudulently purport to have been sent by the Assured but which communications were either not sent by the Assured or were fraudulently modified during physical transit of Electronic Data Processing Media from the Assured or during electronic transmission Assured's Communications Terminal and for which loss the Assured is held to be legally liable.

Although it should be noted that the standard bankers blanket bond, form 24, only provides coverage for "Telegraphic Cable or Teletype instructions or advices..." whereas the Lloyd's electronic and computer crime policy covers telex, TWX and all similar means of electronic communications which includes communications other than "Teletype instructions".

The fifth clause covers the financial institution acting as a service bureau for another bank or customer if it is found to be legally liable for a loss.

INSURING AGREEMENT 5, ASSURED'S SERVICE BUREAU OPERATIONS

> By reason of a customer of the Assured having transferred, paid or delivered any funds or property, established any credit, debited any account or given any value as the direct result of the fraudulent input, the fraudulent modification of the fraudulent destruction of Electronic Data stored within or being run within the Assured's Computer Systems or during electronic transmission through data communication lines from the Assured's Computer Systems into the customer's Computer System while the Assured is acting as a Service Bureau for said customer which fraudulent acts were committed by a person who intended to financial gain for himself or any other person and for which loss the Assured is held to be legally liable.

Coverage is provided for both the bank's loss and the customer's loss. However, the loss of data is not covered during the transmission from the customer to the bank. An additional condition of this clause requires that the person committing the fraud must intend to cause the assured or the Assured's customer to sustain a loss or to obtain financial gain for himself or any other person.

It should be noted that any loss brought about by a change of programs which do not change data would not appear to be covered.

The seventh clause covers fund transfers orally communicated, including coverage when the assured has transferred any funds under fraudulent transfer instructions made over the telephone.

INSURING AGREEMENT 7, CUSTOMER VOICE INITIATED TRANSFERS

By reason of the Assured having transferred any funds on the faith of any voice initiated funds transfer instructions directed to the Assured authorizing the transfer of funds in a customer's account to other banks for the credit to persons designated by the customer and which instructions were made over the telephone to those employees of the Assured authorized to receive said instructions at the Assured's offices and fraudulently purport to have been made by a person authorized and
378 appointed by a customer to request by telephone the transfer of such funds but which instructions were not made by said customer or by any officer, director, partner or employee of said customer or were fraudulently made by an officer, director, partner or employee of said customer whose duty, responsibility or authority did not permit him to make, initiate, authorize, validate or authenticate customer voice initiated funds transfer instructions, which fraudulent acts were committed by said person who intended to cause the Assured or the customer to sustain a loss or to obtain financial gain for himself or any other person.

Special definition

"Customer" as used in this Insuring Agreement means any corporate, partnership or trust customer or similar business entity which has a written agreement with the Assured for customer voice initiated funds transfers.

However, voice initiated funds transfer instructions must be made to a specially authorized employee of the Assured, said instructions must fraudulently purport to have been made by a person authorized or appointed by the customer, as defined, to request by telephone the transfer of funds and the Assured ultimately sustains a loss because the person who gave such instructions was not authorized to make, initiate, authorize, validate or authenticate such instructions.

As with several of the other insuring agreements there must be an intent to cause a loss to the bank or the customer or for the perpetrator or another person to obtain a financial gain.

The revised Lloyd's Policy has also deleted the exclusion dealing with losses caused by unidentifiable employees. This revised

wording now avoids any situation that might arise where the Assured is unable to determine whether a loss, apparently due to an unidentifiable employee, was covered under its bankers blanket bond or its Lloyd's electronics and computer crime policy, the new Lloyd's policy now makes clear that all electronic and computer crimes are covered unless the loss is caused by an identified employee.

Furthermore, Lloyd's has trimmed its questionnaire to eight pages consisting of 30 questions. This is a vast reduction from the original 35 page questionnaire that risk managers said was so detailed that their managements balked at revealing such classified information. [5] Although some risk managers actually find the original London Form to be a valuable risk analysis tool.

In addition to making its coverage broader and the policy easier to read, the underwriters at Lloyd's have done away with the necessity for a security audit of the bank's E.D.P. system. However, the latter may still be required if a given case warrants it.

As a closing comment on the Lloyd's Policy, it should be noted that the revised policy has deleted the automatic reinstatement provision if the entire amount of liability is exhausted and it sets out the maximum aggregate payout per policy period.

> "SECTION 3 LIMIT OF LIABILITY / NON ACCUMULATION OF LIABILITY
>
> The total liability of underwriters on account of any loss or losses or series of losses caused by acts or omissions of any person whether identifiable or not or acts or omissions in which such person is concerned or implicated (and treating all such losses up to discovery as one event), shall not exceed the limit of Indemnity of the applicable Insuring Agreement stated in the Schedule and that if, and only if, there be directly or indirectly no such acts or omissions, the total liability of the underwriters on account of any loss of losses or series of losses arising out of the same event or fraud shall not exceed the limit of indemnity of the applicable Insuring Agreement stated in the Schedule.
>
> Should more than one Insuring Agreement apply, the total liability of the underwriters shall not exceed the limit of in-

[5] *Business Insurance*, February 15th, 1982.

demnity under one of the applicable Insuring Agreements stated in the Schedule and in no event shall each limit of indemnity under separate insuring Agreements be aggregated.

If any loss is covered under more than one Insuring Agreement or Coverage, the maximum payable for such loss shall not exceed the largest amount available under any one Insuring Agreement or Coverage.

Subject to the foregoing, payment of such shall reduce liability for other losses discovered during each year of this policy and shall be applied toward the exhaustion of the aggregate policy limit.

Regardless of the number of years this policy shall continue in force and the number of premiums which shall be payable or paid, the liability of underwriters shall not be cumulative in amounts from year to year or from period to period."

~

The Aetna[6] computer crime coverage is provided by riders that are attached to the bankers blanket bond extending the latter coverage on the basis that it is just another form of robbery or fraud. The following riders are generally attached :

EFT System rider
An independent software contractors rider
A customer communications system rider
A service bureau rider
A telephone voice instruction rider

The EFT rider is not limited to the 5 major funds transfer systems – chips, swift, fedwire, nacha or bankwire II – it is expanded to include proprietary electronic funds transfer systems that are scheduled by the insured in the rider.[7]

The bankers blanket bond is amended to cover losses arising from electronic instructions, advices or modifications thereof having been fraudulently transmitted to, by or on behalf of the insured through a covered electronic funds transfer system provided such instructions were entered at or between the terminals of linked computerized equipment of a scheduled system and were entered

[6] Aetna Casualty and Surety.
[7] Laurence Ochs. Ibid, p. 31.

by a person who purported to represent an institution authorized to use that system.

According to a noted american lawyer,[8] the only potential problem in the EFT coverage is proving that the fraudulent electronic instructions were entered by a person who purported to represent an authorized institution ; often, it may not be possible to determine who entered the instructions.

The "customer communication systems and other instructions" rider provides coverage in instances where a customer has a linked communication system directly or through communications terminals in the Assured's offices or premises. The rider includes automatic teller machines within the definition of "terminal" and attaches the same limitation as the EFTs rider, i.e. proving that the fraudulent electronic instructions were entered by a person who purported to represent an authorized institution.[9] A condition of the coverage is that the assured is legally liable to the customer for the loss.

The "telephone voice communications" rider provides coverage for orally communicated fraud provided that such instructions or advices were made by one person authorized to give such instructions and were electronically recorded by the Assured.

An additional rider provides coverage for those situations where no system, such as the electronic funds transfer system or the customer communication system has been used to penetrate the Assured's Computers. This coverage is a "catch-on" for those situations which are not covered by the EFT rider, CCS rider or the independant computer consultant rider. The rider is directed at those situations where an interloper with knowledge of the Assured's system and the right equipment gains access to the bank's computers.[10] However, one drawback does exist in that instructions must be transmitted to the Assured. If the transmission was made from the Assured who is not an employee as defined, the "on premises" (insuring agreement B) coverage should apply. Although other methods of computer penetration may not be covered. An altered tape that is "put up" on the system by an employee when the alteration took place off premises by a non-employee could raise questions of

---

[8] Laurence Ochs, of Washington, D.C.

[9] Laurence Ochs. Ibid, p. 32.

[10] Ochs. Ibid, p. 32-33.

coverage,[11] likely, where communications are between two computers or terminals within the bank.

IV — Conclusion

Computer fraud insurance is still in its state of evolution and many issues remain unanswered as outlined in this brief review.

The need for this coverage will be in direct line with the individual bank's growth plans and how it intends to make use of computers (a direct product of scientific evolution) to achieve these goals. It is believed to a large extent that many banks have now evaluated that issue and have determined that computers will play a more vital role in their business plans. This in turn will apply more pressure on insurers to tailor fit an insurance policy to meet the demanding needs of banks where the risks of computer fraud are too substantial[12] to overlook or underestimate.

[11] Ochs. Ibid. p. 33.

[12] Ochs. Ibid., p. 36.