N.43267
R.41906

AEAI/RIMS International Conference
October 15-18, 1989
Monte - Carlo

Please respond to

MONDAY, 16TH OCTOBER 1989

SESSION NR 7

COMPUTER SECURITY

COMBATTING CRIME AND MISUSE OF DATA - IS INSURANCE A SOLUTION ?

NICHOLAS SMALL

AEAI

Omer Leroy
UNILEVER
Conference Co-Chairman

Risk and Insurance Management Society, Inc.

gh Loader
'etra Pak
Conference Co-Chairman

You have heard the other speakers talk about the measures introduced by the computer industry to combat computer crime. My task is to explain the range of insurance covers available to provide financial protection should these measures fail.

The two main areas which I shall address are the exposures to fraud and the threatened or actual malicious destruction of systems or data which interfere with normal business activities.

The initial difficulty in discussing computer fraud is defining what it is. For the purposes of outlining insurance cover I would prefer not to work to a specific definition other than to say computers don't commit frauds, people do: the computer is merely a sophisticated manipulative tool which lacks the will and the intelligence to defraud you.

First I would like to breakdown the various methods of using this tool.

- Fraudulent access to the system

  Access in general has become far more important in recent years. Computer systems are now integral to the smooth operation of many companies but in order to exploit their potential access has to be allowed to vast numbers of users. In the 70's it was common for all EDP to be handled centrally with access restricted to those responsible for keying information. Now we see large network systems used by all employees and in many instances by non employees. This requires a strong control environment to ensure that the system is not compromised.

- Insertion of fraudulent data or instructions

  This is the most common means by which companies are defrauded. As new systems have been introduced control procedures have often lagged behind and due to an innocent faith in the integrity of the computer unusual transactions are frequently not spotted until it is too late. Unless there is strict reconciliation of input and output and a clearly established audit trail it may only be by accident that you find out that you have been defrauded.

- Fraudulent alteration of data, programmes or routines

  It is rare for the executive programmes supplied with the hardware to require alteration as these govern the way in which the machine operates. The applications programmes control the maintenance and manipulation of the database and are the programmes which may be amended. Many amendments are carried out for legitimate reasons but it is essential that any amendment is closely scrutinised as a new sub-routine may be patched which can fraudulently manipulate the database. An example would be the instruction to round down odd sums and to credit a new account with the balance. Alternatively the patch could create an artificial environment to give the appearance of normality when in fact a fraud is taking place.

Cont.../2

Although relatively underexploited as a means of defrauding companies this is the area with the greatest potential for causing large losses.

- Electronic funds transfer

I have added this heading despite the fact that EFT fraud is not generally viewed as computer fraud. I am thinking of the use these days by many companies of the facility to instruct a bank to move corporate funds through an EFT system. This has become particularly important in supporting treasury department operations and is vulnerable to transmission of fraudulent instructions.

Instructions might be given through a dedicated P.C. or by telex, telegraph or may be over the telephone.

There have been many examples of EFT fraud described in the Press and the common feature of them all is that a simple method of issuing instructions was put in place with an inadequate authorisation procedure. The recent trial of Alison Anders who attempted to defraud Britoil of £23m is a good example of the potential size of losses in this area.

You may also have read about the man in Scandinavia who opened a series of accounts with various banks investing modest amounts. He told each bank manager that he was moving into their area and was expecting to receive a large transfer of funds following the sale of his old house.

The next part of the plan was to instruct his company's bankers, through the electronic cash management system, to credit these new accounts with approximately £5m. Naturally the banks receiving the funds were not suspicious as he had forewarned them.

- Who should you insure against?

More than 90% of all computer fraud or EFT fraud losses are caused by employees.

They are the people with legitimate access to the system, close understanding of how it works and detailed knowledge of company procedures. Many frauds are made possible by very simple errors in operating procedures that can be exploited by quite junior staff.

It is common to find a complacent attitude to the integrity of the computer system.

- terminals left logged on with no one present
- sloppy attitudes to password control
- lack of control over source documents or hard data

- a touching faith in the output of the computer being correct with no attempt at reconciling this with input.

Sadly it often seems to be true that security declines as security machinery expands.

As Risk Managers it is essential that you ensure that a secure environment is created and that employees believe that they will be caught by the controls that are maintained. However there are always an ingenious few who can circumvent the best laid plans, hence the need for insurance.

As we have suggested that most losses will be caused by employees we should first look at the fidelity cover. There are certain important features that should be considered.

1. Cover should apply whether the employee is acting alone or in collusion with others. There have been circumstances where the employee has supplied the information in order that a third party can effectively break the system.

2. Financial gain should be for the benefit of the employee or any other person or organisation intended to receive the benefit. It would be no comfort if you caught the employee but found that he had been crediting his Grandmother to supplement her Old Age Pension, and then could not claim on the insurance because the employee had made no personal financial gain.

3. Cover should apply even when it is impossible to specifically identify the perpetrator. It may be possible to conclude that one of a group of suspects is responsible but, where the audit trail has been destroyed, unlikely that conclusive evidence will be presented against an individual.

4. Are the limits adequate?

   I am often surprised at the sums insured requested by clients. Multinational corporations transferring millions of pounds with a phone call, dealing in commodities, and sophisticated financial instruments, keeping the organisation afloat on high tech receivables and payments systems seen to be more concerned about the petty cash than the genuine fraud exposure. Today the typical embezzler will have high aspirations, will be in a position of trust, appear diligent and hardworking (he may take few holidays) will have a clear understanding of company procedures and be in a position to cover his misdeeds. It is the people in <u>your</u> position that you should be guarding against.

   I am reminded of the small company whose Finance Director was responsible for the fidelity insurance. He met some resistance when he suggested they buy cover after all 'it could never happen to us'. The company were a little surprised when this trustworthy individual disappeared with large amounts of the companies money, which he had accumulated over the years, but being a company man to the end he had always endeavoured to increase the sum insured to cover the amount that he was stealing.

Cont ../4

Although most frauds are committed by employees it is essential that the third party risks are not ignored. The activities of 'hackers' have attracted wide publicity in recent years but from the viewpoint of fraud you should be concerned with people closer to home. It is rare for companies not to use the services of contract programmers, software engineers and consultants. These people pose a greater risk than employees in that they combine a reasonable understanding of company procedures with a detailed knowledge of the structure of the computer system. This can make companies particularly vulnerable to frauds which result from amendments to applications programmes or patching new programmes especially if the company doesn't have the expertise to check the accuracy and integrity of these amendments.

Another consideration should be the possibility of ex-employees using their old passwords, or those of colleagues, to commit fraud once they have left. It is essential that regular password changes are enforced and particular attention should be paid to deleting passwords of ex-employees and their colleagues.

From the insurance perspective we strongly recommend that third party cover be added to your fraud policies at the same limits and deductibles and with the same carrier. That obviously sounds like self interest but losses arising from manipulation of the computer system can often be difficult to pin down and it makes no sense to run the risk of a claim failing because it falls between the mutual exclusions of 2 insurance carriers.

Although I perceive fraud as the area of most concern, consideration should also be given to covering other criminal acts which have the potential for causing large financial losses to any user of computer systems.

The risks are essentially those of actual or threatened malicious damage and broadly fall into two areas

- physical loss or damage to hardware

- physical loss or damage to software

There are a substantial number of people who have the ability to cause severe disruption to any business which relies heavily on computer systems

The principal motives would appear to be

- financial gain - extortion is the most likely threat. If you don't pay up we will cause your system to shut down or plant a virus or wipe out your database.

Cont.../5

- resentment is a powerful motive. This may be inspired by a political or social movement or may be felt by someone with a grudge against the company.

- hackers derive a lot of enjoyment from the intellectual challenge of cracking the security of computer systems but may also cause considerable damage in the process.

The activities of the 'Chaos Club' in Germany, the posting of sensitive phone numbers and passwords on bulletin boards, and various electronic 'break-ins' are well documented. Indeed it is even possible to buy do it yourself guides on how to penetrate computer security systems. All of this may seem like great fun to the individuals involved but for their victims it can be the start of a painful and costly reconstruction of a lost or damaged database.

The impact on the company can be enormous and will not only involve direct financial loss but interruption to the business and increased cost of working.

Insurance protection is available in 3 main areas:-

1) For loss or damage to computer equipment or the data carrying media a computer policy is available which provides indemnity for

   a) the actual damage

   b) interruption of or interference with the business as a consequence of loss or damage to the equipment or damage to the property within the vacinity of the equipment which prevents or hinders its use whether the computer is damaged or not.

   c) the additional expenditure incurred in avoiding interference with the business

Any company may be vulnerable to physical attack and such a policy can be extremely valuable in protecting what may be regarded as a soft target.

I can give a good example of an incident which happened to one of our Insureds. A man tried to attack his mistress who worked in the computer room. In the course of the attack and with a view to frightening her he fired a shotgun at the computer causing considerable damage.

This policy will provide similar cover for accidental damage or for failure of electricity supply.

I should add that the risk of terrorist attack would be excluded as this should be addressed under a specific terrorism and sabotage policy.

Cont.../6

b) the interruption of business caused by damage or destruction of the software/data.

c) extra expense incurred in conducting business during the restoration period after loss or damage including repair or replacement cost of software and/or data.

In order to obtain cover some insurers have insisted that a survey is carried out, the fees for which can be offset against the premium. Others take the view that an extensive questionnaire will provide sufficient information to formulate terms. Either way, this is a risk whose real impact cannot yet be evaluated and all Insurers are rightly concerned that a sound contingency plan should be in place.

All of the exposures outlined should be regarded as catastrophe risks. Any major fraud or systems failure can cause untold damage to a company, indeed many small businesses may face liquidation. These risks should therefore receive your attention.

We are great believers in the importance of risk management in this area and are happy to work in partnership with our Insureds to achieve the mutual goal of protecting against new exposures which arise from increased reliance on sophisticated computer systems.