N.41907
R.43268

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

Please respond to

MONDAY, OCTOBER 16, 1989

SESSION NR 7

COMPUTER SECURITY

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

ERIK NORBERG

AEAI

Omer Leroy
UNILEVER
Conference Co-Chairma

Risk and Insurance Management Society, Inc.

gh Loader
Tetra Pak
ce Co-Chairman

How an EDP man approaches Information Security problems, especially computer crimes and misuse of data.

GENERALLY

Information security is one type of security within the EDP area. If we look at the development of the area we can understand the different levels of security.

In the 60's we only had **computer security**. This was security for the computer such as fire and water protection and a locked computer room.

In the 70's, when the on-line technique was introduced, **data security** became the popular expression. The above mentioned methods were then supplemented with the use of passwords.

In the 80's we talk of **information security**. We regard information as an important asset and we guard it with a variety of techniques suitable to the type of information we handle. Information security applies whether the information is stored on data media, paper or in another way.

Please observe that the meaning of computer security, data security and information security may vary between countries and organizations.

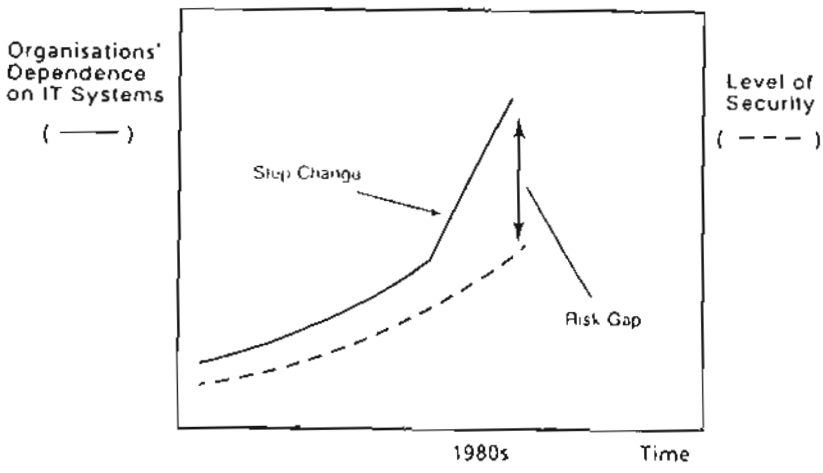
CURRENT SITUATION

The Information Security Risk Gap

During the 80's information security has gradually increased. But what has increased much more is the organizations dependence on IT (Information Technology) system, due to the introduction of new techniques such as EDI, (Electronic Data Interchange), MHS (Message Handling System), CAD/CAM (Computer Aided Design and Manufacturing), JIT (Just In Time technique), etc. This means, that a security risk gap has developed during the decade.

Picture 1.

The Information Systems Security Risk Gap

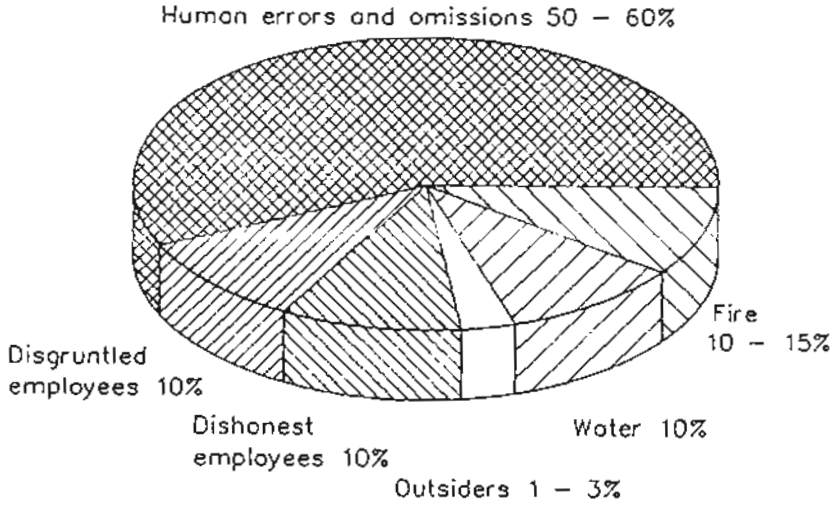


Threats

The next picture shows a merge of the result from different American and European investigations coming almost to the same result.

Picture 2.

THREATS AGAINST INFORMATION SYSTEMS SECURITY



As seen in the picture the big risk is the insiders. In many companies this has not been fully understood and measures are not taken accordingly.

Outsiders are a small part of the threat. However, this may vary considerably depending on the line of business. For example, companies handling many payment transactions are more vulnerable and so are companies with large R&D investments, such as in the pharmacy industry.

Virus attacks and hackers and crackers are minor problems, even if they are popular themes in the media. They are included in the outsiders' group.

Once again, insiders are the big risk. And among them, the terminal users are the most common reported criminals. Another group that could create problems is the EDP staff with a combination of application knowledge, technical knowledge and high access rights. One example could be an EDP manager at a small site. The reason why this group is problematic is that they have the possibility to erase all tracks of their crime in audit trail and logs.

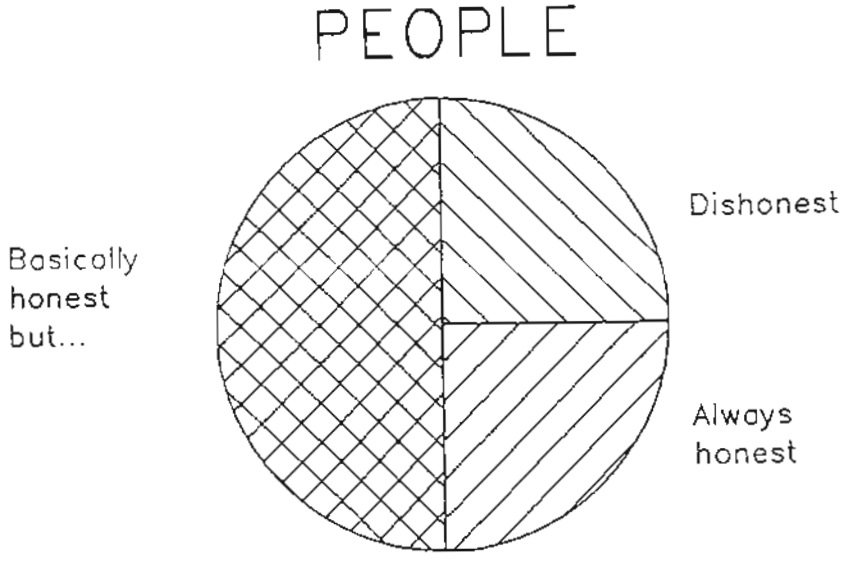
Honesty

What is the situation about honesty?

A small group of people is always honest. Another small group is dishonest.

The large group is basically honest but will grab an opportunity to enhance their standard of living if they consider the risk of being caught minor.

Picture 3.



How do we select people for the sensitive EDP positions to get the always honest ones? In USA both polygraphs, that is "lie detectors", and paper-and-pencil honesty tests are used. In Europe the use of such tests is rare, due to legal obstacles and tradition.

Disgruntled employees

Dissatisfaction can arise both in EDP and in the user departments. It is easier and more important to avoid in EDP as:

- the ratio of users to EDP staff can be between 15:1 and 50:1.
- the crimes committed by EDP staff may cause greater damage and may be more difficult to expose.
- in EDP, as a specialist department, it might be possible to give some extra benefits to keep the staff satisfied.

Common Computer Crime Methods

On this table you can see the most common crime methods. The areas for the crime come from a sales company.

Table 1.

Methods	Areas	Objectives
Altering data	Accounts payable	Money
	Accounts receivable	Money
	Payroll	Money
	Sales order processing	Money or products
Misuse of authorized computer access for unauthorized purposes	Various	Trade secrets or to run own programs
Theft of listings, tapes diskettes, or "dumpster diving"	Various	Trade secrets
Impersonation	Various	Trade secrets or to run own programs
Physical attack	Computer centre	Stop operation
PC theft	Stealing and selling	PCs or money

Crime Ratios

According to estimates made by US computer crime specialists we have the following situation.

- 1 out of 100 computer crimes is exposed
- of these 1 out of 8 is reported to the police
- of these 1 out of 33 is sentenced to imprisonment.

Strong and Weak Areas

Which are the strong and weak areas in Information Security?

According to an investigation initiated by the commission of the European Community, the mainly good areas are where we have long experience and a defined responsibility.

These areas are:

- Physical security
- Computer operations
- Equipment
- Network operation

The bad areas are those where security has earlier not been focused and where responsibility often is not defined, such as:

- Micro computers
- Contingency planning
- Telecommunication
- System maintenance

ACTIONS TO BE TAKEN

The answer to "what actions are to be taken to combat computer crimes and misuse of data" is that this is a part of the information security work and must be handled/organized as such.

Main Activities

The main activities are:

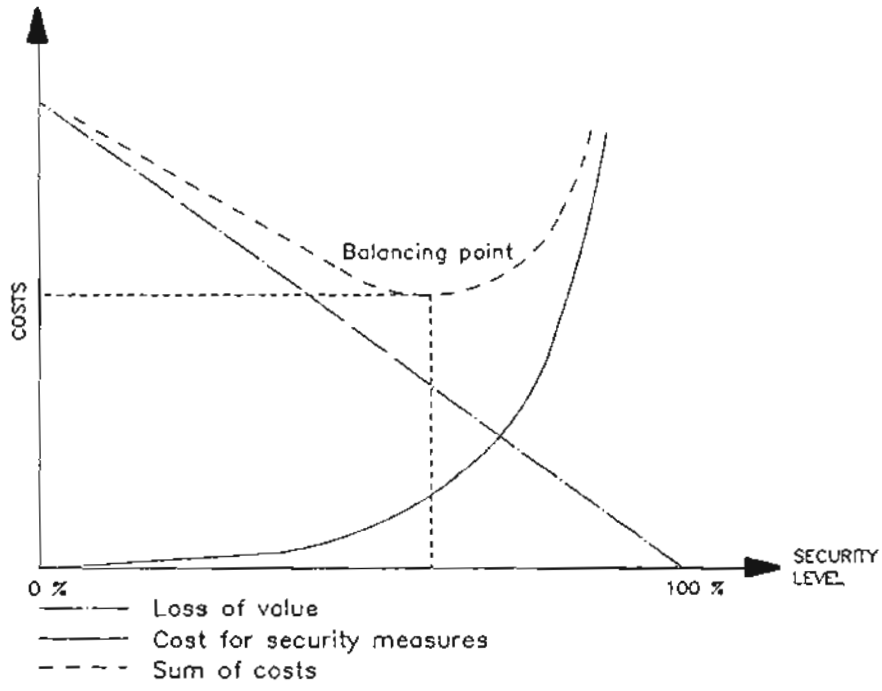
- Deciding the level of security required
- Creating awareness
- Creating a policy
- Creating standards
- Organizing the security work
- Taking security measures physically and logically
- Contingency planning
- User training

Some of these main activities are outlined below.

Level of Security

Deciding the level of security required calls for a risk assessment and finding the balancing point of the sum of losses and costs for security measures. In fact this is not one balancing point but one for each area of security.

Picture 4.



We also have to decide where to use preventive and corrective measures or a combination. Often the preventive methods are more cost efficient.

Awareness

Awareness about the risks and the need to reduce them must be created on all levels of the organization, starting with the top and middle management as "Computer security requires management commitment".

Policy

When creating a policy, the main statement should be followed by special policies in different areas such as

- Information classification
- Microcomputers
- Data communication

For the main statement I find General Motor's policy to be one of the best. "Information is a corporation asset and all employees are responsible for protecting that asset from unauthorized access, modification, destruction or disclosure.

Security Measures

Here follow a few examples of how potential criminality from insiders can be reduced. The first line of defence is to avoid letting criminals into the organization and the second is to prevent them from carrying out their plans.

- To reduce the risk from dishonest employees improve the methods for personnel

screening.

- To reduce the number of disgruntled employees (especially within the EDP function) increase the awareness among managers. Implement a good, market oriented salary structure. Create motivation.

- To reduce the possibility for terminal users to cheat the company, use more programmed controls.

- Use a good access control system, that limits the access to the information, which each employee needs for his job. Use passwords difficult to guess or calculate. Passwords should be altered frequently.

- If human errors and omissions are to be avoided, routines, documentation, education and training are essential.

There are a number of security methods against **outsiders** that can be used. Some of them are also useful against insiders. Here some examples:

- Use encryptation of disk.

- Use encryptation of data communication.

- Use call back devices wheren a stationary micros start data communication with a larger computer.

- Use of a good access control etc, as mentioned above.

- Alter the passwords frequently.

- At dial-up connections, use of handheld random password generators.

- Do not allow games or software from not secure sources on production computers or networks.

- Keep computers used for accessing Electronic Bulletin Boards or other risky environments seperated from own networks.

- Use "antivirus" software.

Some products in this area are fancy, expensive and rarely used, such as biometric access control. Also a high level encryption system is expensive because of the additional workload it creates on the computers.

Many of the methods will create additional work and trouble for users and EDP.

CONCLUSION

Combating computer crimes and misuse of data is an integrated part of the information security work. The job has to be organized, planned, and carried out carefully. Among many success factors two ought to be stressed specially:

- Balance the measures to be taken against the risk assessment.

- Avoid overdoing, especially regarding the external risks.