COMITÉ EUROPÉEN DES ASSURANCES

SECRÉTARIAT GÉNÉRAL
3bis, rue de la Chaussée d'Antin F 75009 Paris
Tél. : +33 1 44 83 11 73 Fax : +33 1 44 83 11 85
Web : cea.assur.org

DÉLÉGATION À BRUXELLES
Square de Meeûs, 29 B 1000 Bruxelles
Tél. : +32 2 547 58 11 Fax : +32 2 547 58 19
Web : cea.assur.org

PROPERTY INSURANCE COMMITTEE

Computer Crime

1. Introduction: What is computer crime?

There is no official definition of the term computer crime. In abstract terms, this phenomenon became a real topic only about twenty years ago; computer crime is considered to be a *malicious,* intentional, *harmful act* of a *person* who is trying to obtain *financial gain* or to satisfy *non-financial goals.* This act is carried out through the use *of data processing equipment* namely by the deletion, a*lteration or insertion of data* in an EDP system or during data transmission. Until the Internet had gained major importance, computer crime for non-financial goals was practically non-existent. Traditionally, a distinction between active and passive fraud is made. By active fraud, we understand a situation in which a criminal is actively looking for gaps in the security system and when the opportunity arises he commits a crime to obtain financial profits or to fulfil other goals for himself. By passive fraud, we understand a coincidental detection of a gap in the security system. The person who has detected this gap remembers it only in times of private troubles and commits the fraud months or even years later.

In fact, every company can be the target of a fidelity crime. The exposure can be increased by numerous factors such as on the company side: unclear company policy and goals, unclear organisation, responsibilities, difficult financial situation and on the employees' side: demoralisation, frustration, envy, bad working climate, personal and family reasons as well as financial problems again. But the company is not only endangered by the malicious acts of its employees. External parties providing services as well as all third parties are also in a position to commit such an act as potential perpetrators.

In fact, the moral hazard that constitutes the basis for the existence of a phenomenon like computer crime seems to be huge. A study carried out in Germany stated that only 20% of those interviewed claimed to be completely honest, 10% confessed to be dishonest sometimes and the overwhelming majority of 70% could imagine being dishonest under certain negative circumstances, such as financial problems, frustration, good opportunities.

2. The current situation of computer crime

The United Nations is so concerned about the development of Internet criminality that it has already taken up this topic several times. And when we talk about computer crime today, we mean primarily crime committed through the Internet. A German study stated that, in 1999, in 57% of all cases of intrusion by externals to computer systems, the Internet played a role (in 1996, this was only 37%). The person responsible for drug control and crime prevention in the UN even attaches to this phenomenon a quality similar to crimes against humanity. According to him, the Internet is continuously gaining importance as far as its role in international drug commerce is concerned. A viable scenario sees the Mafia carrying out all money laundering through the worldwide net in the future. It is felt that it is high time to elaborate an international jurisdiction for this global - and up to now scarcely controllable - problem.

The German Ministry of the Interior is also demanding international co-operation against hackers and cyber-terrorists. It fears a new wave of blackmailing in society created by opportunities produced by the Internet.

In the United States, computer crime is outpacing "cybercops". The FBI saw a 39% increase in computer crimes in 1999 compared with the previous year. The problem is that the nation has only several hundred high-caliber forensic computer experts. In theory, the FBI and Justice Departments have dozens of jobs for computer investigators but can barely compete with private firms offering salaries which are twice the government paycheques. The FBI hires experts and trains them on the condition that they stay for five years. In reality, they often cannot keep them for this period of time. Thus, only a handful of police and sheriff's departments have the money to support squads of "high-tech" investigators.

The theoretical consequences of an act of computer crime could be: the *loss of financial assets;* the *loss of property* (this could comprise equipment, goods, raw materials as well as goods manufactured by the insured or in the process of manufacture); *the loss of intellectual products.* Such intellectual products could be software programs, building construction plans, statistics etc. Beside the loss of these items, competitors could gain a technological advantage and a time advance and enter the market with a new product earlier than the company which originally elaborated the intellectual product. The latter is likely to lose market share and might also have problems to maintain its positive image. Also, *the loss of computer time and use* caused by fraud was always a topic. Here, a theoretical loss can be calculated by multiplying the period of time in minutes where unauthorised use of computer time was carried out with the EDP-budget per job-minute.

The FBI estimates the average damage per criminal act (unlawful intrusion in computer systems of enterprises) at USD 500,000 and the total damage in the USA due to cybercrime at 266 m USD for 1999. Specialists hold the view that this number is most probably underestimated. The market research company Datamonitor thinks that unlawful intrusions into computer systems of enterprises cause worldwide damage of approximately USD 15 bln. per year (1999). Exact figures are difficult to evaluate but it is most probable that the cost of damage through cybercrime doubles every year. Thus, taking the « love bug » into account, a figure of USD 30 bln. for the current year would be realistic.

3. The role of the Internet

The Internet created a whole new class of criminals. Through the introduction and use of the Internet, closed company EDP-systems have become systems open to attack from outside the company. In the majority of cases, computer crime is nowadays Internet crime. Via the Internet, harmful programs which are contaminated with viruses are sent all over the world and cause enormous damage. E-commerce is not only commerce with usual goods which contribute to our own lifestyle and convenience at lowest prices. It also means dealing with drugs, illegal medicine and people. Through the Internet, contents which are an offence, such as articles containing racial hatred topics or illegal sex issues, are freely distributed. The perpetrators can hardly be identified and, if so, they are often situated in countries where there are no extradition treaties. It is hardly possible to prosecute these people or even investigate their crimes.

Hackers and crackers (criminal hackers) are increasingly manipulating the homepages or websites of companies and modifying information. This page hacking activity can lead to disparagement of the company or even to a display of incorrect prices for products sold. The « repair » of the hacked page often leads to downtime in activity. Additionally, so-called page jacking has become a problem. In such a case, a hacker manipulates the IP address of a website so that regular access to this website is no longer possible or at least impaired. This act can also result in a downtime loss for the company in question.

4. Different qualities of computer crime

« Traditional » cases of computer crime

In the traditional case of computer crime, data and the data base is often stolen. They contain the names and addresses of important clients. This problem can be found in marketing departments of big groups, in personnel departments where data for job candidates is stolen and in high technology firms. Often these are cases of industrial espionage committed by competitors or by own employees who take the data with them before leaving the company, often in order to start their their own businesses. The percentage of cases ignored by the public is extremely high, estimated at 80% - 90%. Hardly any company wants to talk about this sensitive point, about the gaps in their security systems in order not to harm their perfect image with the public.

There follows a short survey of cases of computer crime. These so-called traditional computer crime cases illustrate very well the field of computer crime before the Internet era.

In Germany, a warehouse manager manipulated the software program of his company's EDP system so that all delivered spare parts were shown with false prices. He pocketed the difference in price himself which was very much to his advantage. The result being that his company suffered a loss of more than **EUR 150,000.**

The programmer at one bank rounded off all figures which appeared after the decimal point when carrying out money transfers. Within a short space of time he was the richer by a few hundred thousand Euros. Those he had embezzled had not noticed that they had not been credited with the full amount due to them as the sums manipulated amounted to only a few Eurocents in each case.

A number of employees at a company in the USA used the firm's EDP unit for private purposes. By means of the highly specialised software program they were able to carry out extremely complicated constructional design work and statistical calculations for private tenders. Quite a substantial portion of available computer time was spent in this manner. Company management only discovered this illicit use of computer time a few months later.

An executive at one company opened up dummy accounts for himself and a number of his accomplices. Money belonging to his employer was illicitly transferred to these accounts via program manipulation without leaving any evidence. However, embezzlement was discovered when the programming documents were mistakenly returned to another computer employee who had nothing to do with computer fraud. The entire loss ran to EUR 350.000.

Mainly from Italy, we have knowledge of a whole series of these traditional computer crime cases which occurred in the end of the 80s. Mostly bank employees found ways to transfer money from clients' accounts into their own bank accounts often abroad. We know from a case in Naples, where in 1986 a bank employee stole EUR 2 m by manipulating the accounting system. At the same time, a bank employee in Venice transferred EUR 0.5 m into a secret bank account in Switzerland. Another employee in northern Italy manipulated the balances of debited accounts so that they showed immense sums. He and his accomplices then withdrew the money from these accounts by using counterfeited checks. A group of state officials in the Rome region manipulated their own salaries in 1988 by adding enormous extra hours and expenditure for continuous long travel throughout Italy so that the salaries were doubled or even tripled.

Coinciding with an increased alertness and the implementation of control mechanisms, the frequency and the damage caused by such traditional computer crime cases from the early years of computerisation has diminished a lot. With the introduction of the Internet, they are no longer the major topic when talking about computer criminality.

« New » type of computer crime: Virus attacks and acts of hackers

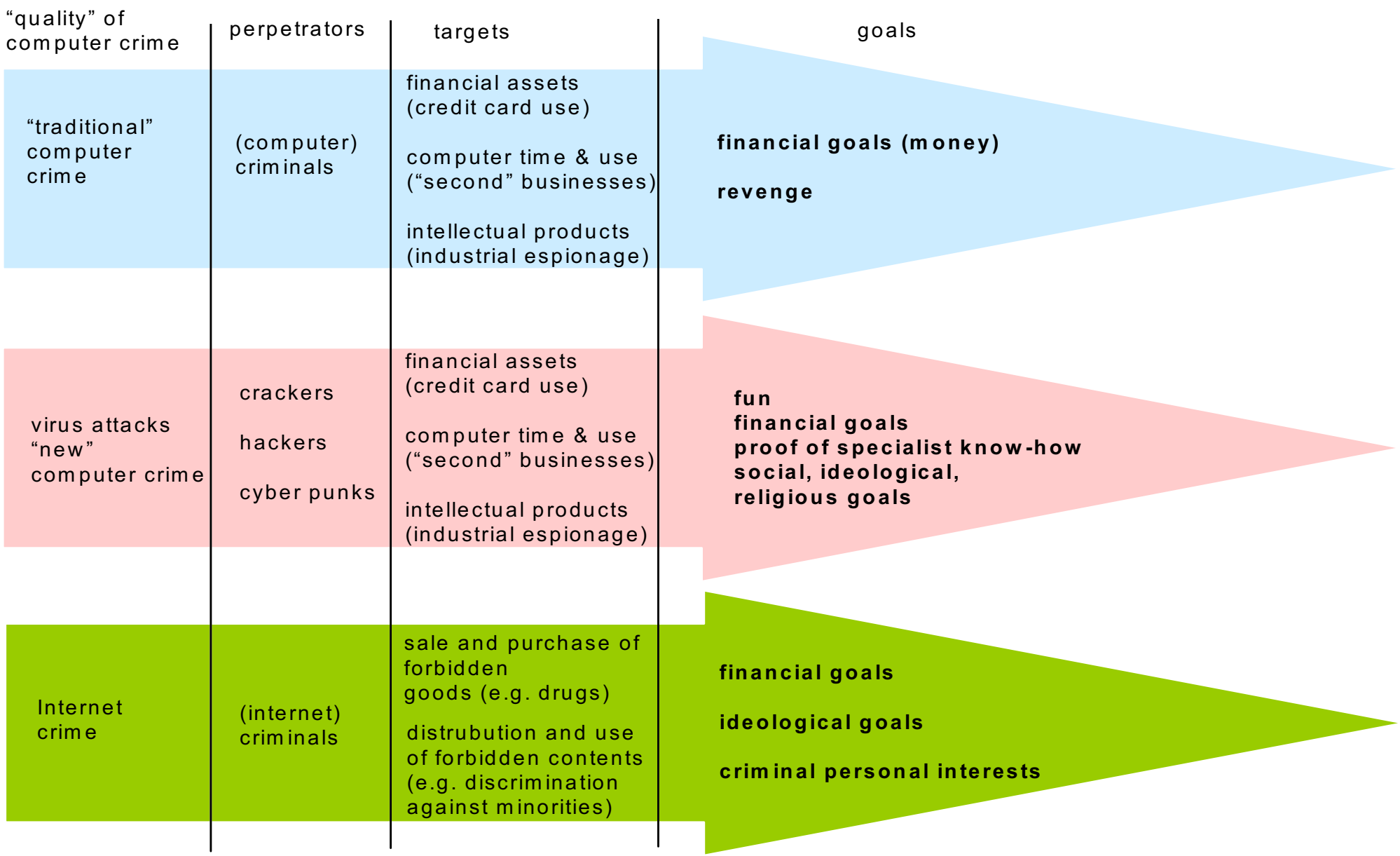
As criminal acts through virus attacks gain an ever increasing importance, a whole chapter is dedicated to this problem (cf. chapter 5). Hackers enter the computer systems of enterprises and institutions for various reasons. The classical definition of computer crime with the mere goal of stealing money is not sufficient anymore. Hackers often want to prove their specialist expertise and compete with their fellows by intruding into ever better protected systems. Beside this competition and

fun element, so-called "cyber-punks" are spreading viruses and entering systems for social, ideological and religious goals. Notwithstanding the above, criminal hackers (so-called « crackers ») are continuing to intrude into systems in order to obtain money and other financial assets. This type of computer crime is not really new, but has gained enormous importance, coinciding with the popularity of the Internet. There is, however, a type of computer crime which only began to emerge with the existence and spread of the Internet.

Internet crime

Internet crime is a totally new field of computer crime which was practically non-existent some years ago. The Internet has become a marketplace for the sale and purchase of goods and service which cannot be dealt with in a legal way. ln this context, we think of illegal drugs and medicine, of weapons and even of nuclear material. But not only goods, people also can be booked through the Internet. Beside partners for illegal sex issues, you can hire murderers, terrorists and soldiers. Furthermore, racial hatred and radical political and religious views can nowadays be spread all over the world in seconds through the Internet.

The problem, which is inherent in the third type of computer crime, is the different legislation in the countries all over the world and the fact that even if governments wanted to control the contents of the Internet more strictly, the private sector does not normally support them in order not to lose business.


"quality" of computer crime
perpetrators
targets
goals
"traditional" computer crime
(computer) criminals
financial assets (credit card use)
computer time & use ("second" businesses)
intellectual products (industrial espionage)
financial goals (money)
revenge
virus attacks "new" computer crime
crackers
hackers
cyber punks
financial assets (credit card use)
computer time & use ("second" businesses)
intellectual products (industrial espionage)
fun
financial goals
proof of specialist know-how
social, ideological, religious goals
Internet crime
(internet) criminals
sale and purchase of forbidden goods (e.g. drugs)
distrubution and use of forbidden contents (e.g. discrimination against minorities)
financial goals
ideological goals
criminal personal interests

5. The role of virus damage in the field of computer crime

Until the beginning of the 90s, losses through computer viruses were always a more theoretical case of computer crime and the damage caused by « traditional » types of computer crime was of much more importance and also heavily published by the mass media. When the Internet began to gain popularity, the speed of distribution of worm-type viruses grew so much that damage has become inevitable. 45,000 types of active viruses are known today. They can be distinguished according to their targets and their way of acting.

Many experts consider a virus to be a catastrophe problem today, even more menacing than flood, storms and earthquake because it is not restricted to a geographical region. The most harmful and widest-spread virus, which we have got to know so far is the « I love you » virus, also named « the love bug ». To a virus, such as the « love bug », the whole world is exposed in one event.

« I love you »

It is not clear what goals were lying behind the virus attack with « I love you » in May 2000. The virus affected computers that used Windows 98 as well as Windows 2000 operating systems and those on Windows NT4 and Windows 95, if they had Visual Basic Scripting engines. It looked like a text file and therefore people opened it. After a series of processes, the virus finally replaced all documents in certain categories of files with itself, so a user trying to open a photograph or music file started the virus all over again. The data in the files was lost as a result. The computer virus caused economic damage which is estimated at between USD 5 bln. and USD 15 bln. (EUR 5.3 bln. to EUR 15.8 bln.) within the first five days after its release. This would be mostly due to production hours lost and not due to corrupt files. The insurance loss, however, is said to be tiny compared to this sum. Coverage against business interruption after virus attacks is not widespread yet and most of the Internet users were not aware that virus attacks could have severe consequences which were unknown until then. Even major global players such as AT&T, Nestlé, Merrill-Lynch, Siemens and Delta Airlines have been struck by this virus. The biggest losses were caused by the blocking of mailboxes and the costs in order to put the hundreds of thousands of infected PCs back to work.

The « love bug » in figures:

Estimated cost of virus damage due to « I love you »	USD 5 - 15 bln. World-wide
Number of computers that have been affected by the virus	1,500,000
out of this: In the USA	600,000
Percentage of American enterprises that have been struck by the love bug	26%
Percentage of American enterprises that took preventive measures (closure of mailboxes, activation of anti-virus software)	47%
Insured damage due to the « I love you » virus in Europe	> EUR 2,500,000

Before the « love bug » came into existence, the world had only known one virus which was most harmful and globally active. « Melissa » raged for several months and even hit the renowned German insurer, Gerling.

« Melissa »

In November, 1999, the feared Melissa virus entered the computers of the Cologne-based insurance group, Gerling. This had the effect that the PCs automatically sent out 50 contaminated e-mails each. Amongst the addressees were even customers of the insurance company. E-mail communication inside Gerling had to be stopped. The cost of decontaminating the systems from the virus was said to be around EUR 50,000. The loss of image can hardly be quantified. Inside Gerling, the chain reaction started with an employee of a Gerling London office who received an infected e-mail. Unsuspecting, he opened the attached document by which the virus could spread. Afterwards, Gerling improved its computer security a lot.

Since that time e-mails coming from external sources can only get into the system after having passed online virus scanners. The Melissa virus was known to be in existence as early as April 1999 and led to a whole series of losses in different countries for several months. Melissa caused more than USD 80 m damage in the entire world.

Cases which are similar to virus effects

Similar to virus attack are cases where prestige servers have been overload with rubbish e-mails with fake questions and orders. Amazon and Yahoo have already felt such types of attacks blocking their servers totally. This leads to a so-called *Denial of Service Interruption loss.* During the past few years, innovative Loss of Profits insurance concepts emerged in some mature insurance markets worldwide. They included cover against loss of income after non-physical damage (such as contamination by computer viruses and blocking of service capacities through Worms and Trojan Horses). Now that insurers and reinsurers have started to take a more strict and risk-minded approach to the exposure which is inherent in such covers, these innovative concepts are step by step disappearing again. Up to now, specialists have failed to assess a PML figure that is substantially below 100% as far as lost profits after virus damage is concerned. Thus, the exposure of such covers is currently assessed as being enormous and the risks as not insurable.

6. Influence of computer crime on the development of e-commerce

Nowadays, all specialists agree that the development of the e-commerce sector, which is without doubt nevertheless prospering, is impeded by computer criminality. A substantial percentage of potential buyers around the world forego purchasing goods and services via the Internet because they do not want to reveal their credit card numbers. There have been cases of misuse of credit card numbers that had been displayed in e-commerce transactions in nearly every industrialised country.

Credit card numbers nowadays are treated like merchandise and sold as well as exchanged over the Internet. The goal is to make it more difficult for the police to trace where and by whom the cards have been misused. The credit card numbers have not necessarily been stolen in the e-commerce process but could also been copied by a waiter in a restaurant who spreads them now via the net. Even more often than credit card numbers, the weak points of governmental authorities' and private companies' computer systems are traded. There is a widespread search for experts who can intrude into various systems.

Switzerland has a leading role amongst the European countries as far as e-commerce is concerned. The average Swiss spends four times more than the average European on online shopping, twice as often as in other European countries bank transactions are carried out through the Internet. On the other hand, the Swiss are the most fearful amongst the European as far as credit card misuse is concerned. This also holds true for companies which sell their goods and services through the net. Already today this extreme fear is an essential obstacle in the further development of online shopping in Switzerland. Prognoses for online business paint a pessimistic picture for the future of Internet transactions in Switzerland, if the security of the net cannot be assured in the future.

In Germany, complaints against payment via the Internet are increasing tremendously. Credit card companies estimate the part of embezzlement through the Internet as already 10% of all credit card crime. Often, the credit card company takes over the costs for misuse of credit cards of their clients for payments.

In the past year, Italy saw approximately 800,000 purchase transactions online with a prognosticated doubling to 1.5 m within the current year. Compared to other countries, the rate of credit card misuse in Internet shopping is small in Italy. Only one in 20,000 transactions is manipulated compared to one in 550 in the rest of Europe. In order to maintain this favourable rate, Italy has created new teams of electronics specialists inside the police, the finance administration and even in the military.

7. Prevention and protection measures

The G 8 association (the seven most important industrialised countries plus Russia) attaches great importance to the role of cybercrime. In a conference, it regretted that governments alone cannot solve the problem of this fast developing crime sector. The missing link is private industry, mainly Internet providers like AOL who rely in the force of the free market with its auto-regulation. France wants to extend the rights of Interpol as far as the fight against cybercrime is concerned. The French police have established a central office for the fight against criminality in the field of information and communication technology (OCLCTI). Its task is to carry out high-level justice research in order to find traces of cyber criminals. Based in Nanterre, the office is situated within the central organisation of the justice authorities. Germany has also founded a similar institution.

The credit card institutes are constantly trying to improve their security systems. New encryption technologies, such as SET, or additional chips are meant to identify in a virtual world the card user as the real card owner. SET is the abbreviation for Secure Electronic Transaction. It consists of a protocol for secure payments by credit cards. It was developed jointly by Visa and Mastercard as a successor to their own individual tools. CyberTrust is the brand name for electronic cash transactions using the SET encryption standard. The big credit card institutes co-operate with IBM, Netscape and MSFT. In the near future, the CyberTrust software should be integrated in the WebBrowser. Information technology specialists, however, are sceptical. They claim that up to now each and every code has been able to be cracked.

One additional protection is the existence of a TAN (transaction number). This is a several digit additional PIN from a special list which has to be added to each new transaction. This ever changing code is only known to the bank and the owner of the bank account. TANs are a classical measure in order to prevent the data of a transaction from being copied and used again (replay attacks). Even in cases in which the PIN is stolen, the perpetrator would have to procure for himself the currently valid TAN in the list in order to pretend to the bank that he was making a real transaction.

One efficient security measure which is in use already today is that credit card numbers in general do not go directly to the virtual shop where the customer is going to buy something but to a so-called virtual POS which is run by banks and authorises the payments due.

Neil Bolton, manager of insurer Hiscox Technology, said in Lloyd's List that the best way of preventing damage caused by strangely-titled messages was always just to delete them. Other elements of a comprehensive protection programme are the continuous education and training of the staff as far as their alertness is concerned and the regular update of anti-virus software as often as possible. Unfortunately, on average no more than 5% of the total EDP budget is dedicated to security.

Anti-virus software currently only offer protection against 50,000 known types of virus. A magic programme, detecting all existing (and furthermore all not yet existing viruses in the future) is not in sight. Existing anti-virus programs mostly fail in detecting viruses of new and unknown types.

8. How to insure against computer crime

Currently, the insurance facilities for what we call « traditional » computer crime are numerous. This not only refers to engineering insurance lines, but also to other branches of insurance (cf. fidelity covers). Different forms of so-called data and software insurance covers as well as specialised computer crime covers, popular and well-known especially in France under the name « fraude informatique », can cover against the effects of theft of financial assets, computer time and against financial loss through industrial espionage.

Also for the « new computer crime » classes that have emerged through the increased popularity of the worldwide web up to a few months ago the markets offered special insurance capacity. Amongst others, Lloyd’s of London, some

American insurers and TELA Versicherung AG, a German specialist reinsurer which has left the market in the meantime, were forerunners in granting such innovative and comprehensive coverages for users of EDP-systems.

In the recent past, however, capacity has decreased dramatically because reinsurers now take a more restrictive approach to the insurance of computer viruses which can spread in an uncontrollable way through the internet. Some of the biggest reinsurers worldwide grant no capacity for such virus damage anymore. One reason for this is the experience with the Y2K problem which did not cause a lot of damage to the computer industry but could have done so acccording to reinsurers. They suppose that a spread of viruses through the Internet accumulates to create enormous damage in a very short time and leads to exposure which is far from being assessable. Contrary to natural peril risks, such as earthquakes or windstorms, the accumulation zone cannot be defined, it is the entire world. Up to now, experts have failed to make a reliable PML estimate for the most sombre virus scenarios. The same holds true for similar loss cases, caused by so-called « Worms » or « Trojan Horses », programs which re-produce themselves automatically and can totally block computer activity by devouring computer capacity (so-called denial of service attacks).

It goes without saying that the current situation is unsatisfactory for the buyers of insurance cover as far as the availability of coverage is concerned. Therefore, research carried out by insurers and reinsurers in the markets is currently being intensified to find a solution to cope with the actual non-insurability of the virus risk. Until such a solution is found, the user himself must ensure maximum protection of his systems by using up-to-date virus scanners, firewalls etc. and by educating the staff in simple behaviour patterns such as not opening e-mails from an unknown sender.

9. The future of computer crime

The experts in new technologies paint a sombre picture of a future in which cyber-terrorism might flourish. They even say that after chemical and bacteriological weapons and nuclear risks, this could be the third major threat to the world of tomorrow. In this context, attacks mainly against vital infrastructures are feared, such as air traffic control, nuclear power stations, electricity supply or the railway system. In the small range, scenarios in which software in hospitals is manipulated in order to murder a patient can be imagined.

10. Literature

1. Lloyd's List, 12.5.00 (Great Britain)
2. Facts No. 26, 29.06.2000 (Switzerland)
3. The Times, 11.01.2000 (Great Britain)
4. TELA Versicherung AG, Munich; own research (Germany)
5. Frankfurter Allgemeine Zeitung, 30.06.2000 (Germany)
6. Financial Times South Africa, July 2000 (South Africa)
7. International Herald Tribune, Zurich, 05.05.2000 (U.S.A.)
8. Tribune, 18.05.2000 (France)
9. Le Monde, 17.05.2000 (France)
10. Handelsbiatt, 24.11.99 (Germany)
11. Focus 45/1999 (Germany)
12. Die Welt, March 2000 (Germany)
13. Le Journal des Finances, 15.05.00, (France)
14. Tribune, 16.05.00 (France)
15. Handelsblatt, 15.2.00 (Germany)
16. Il Gazzettino, II Corriere della Sera, la Repubblica, various articles from the end of the 80S (Italy)
17. Zeitschrift für Versicherungswesen, Mai 2000 (Germany)

Wolfgang Wopperer, February 2001

g :ab\ab2001\ab1028e