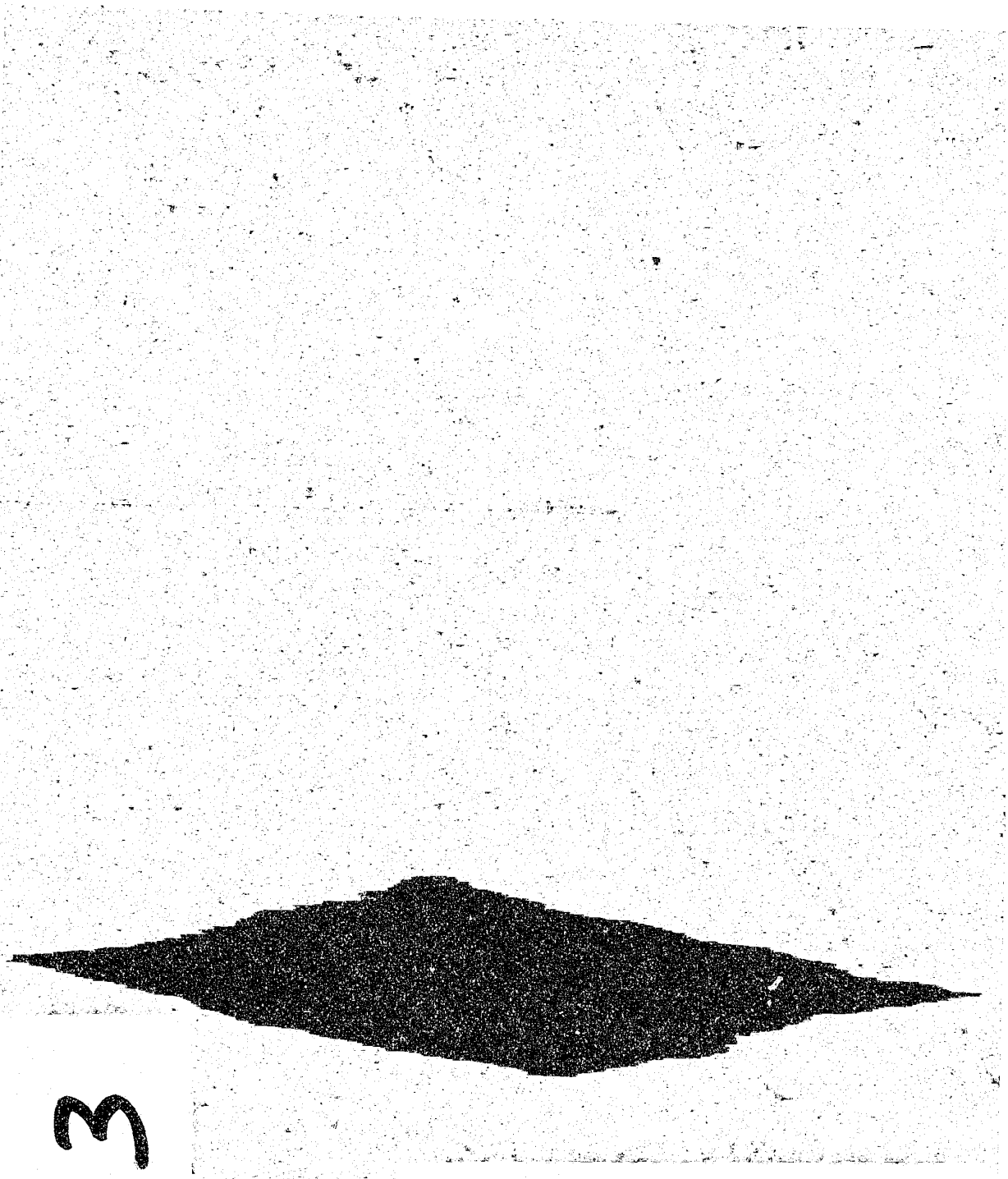


U.S. Department of Justice
National Institute of Justice

International Summaries

A Series of Selected Translations in Law Enforcement and Criminal Justice

National Institute of Justice/NCJRS
NCJ 99853

From Sweden

Computer Technology and Crime

To reduce vulnerability to computer crime, opportunities to illegally access the system need tc be reduced.

By Arthur Solarz

This report describes evolving forms of computer crime in Sweden and discusses traditional criminological theory on causes and motivation of crime as it applies to computers. Topics covered include:

- The history, development, and trends in automation in Sweden.
- Automation as it affects social structures and as a potential basis for crime.
- Definitions and understanding of computer crimes.
- Factors influencing the vulnerability to and the opportunity for computer crime.

The report presents two empirical studies of computer crime involving both embezzlement and theft. The studies review who engages in it, what they take, and how they take it. Results suggest implications for prevention. Emphasis is given to reducing opportunities to commit computer crime.

Sweden is one of the most automated countries in the world. Automation is common in the public and private sectors and is used in budgeting, financial and personnel planning, bookkeeping and auditing, retail applications, sales prognoses, publishing production applications, and more. In 1983, 68,400 modems were registered in the country; by 1987, this figure is expected to reach 126,500. Nearly half of all Swedish companies with more than 500 employees have their own large data systems, personal computers, and word processing systems.

Automation and criminality

The effects of automation in terms of criminality are not clearly understood and can cover many aspects of life. For instance, automation in the workplace commonly causes a lower demand for personnel and, although automation has been linked to greater growth for some companies, it causes a "jobless growth." It increases, therefore, the likelihood of greater unemployment and expanded leisure time. These changes can relate to criminality and to significant changes in lifestyle.

Another aspect of automation is the increased ability of companies to employ persons who work in the home rather than the office. Linked by telecommunications and working at terminals, these employees are far removed from the controls of the workplace. (At the same time, working at home may affect the incidence of daytime burglaries.) Further, home computers and the exchange of information and retrieval of information by household members can influence relations among family members, since parents may no longer be the primary source of children's information, thereby disturbing some of the natural bonds between parents and children.

Computer crime—understanding and definition

The concept of computer crime is not yet well established, and its definition differs among disciplines. The legal community describes computer crime as a formally illegal act for which sanctions must be prescribed. The criminological community describes computer crime in terms of its causes, motivations, and characteristics.

The literature is not in agreement: see Edelhertz (1977), Bequai (1978), von zur Muhler (1975), Parker (1980), Scholberg (1983), and the Computer Abuse Research Bureau at the Caulfield Institute of Technology in Australia (1980). Figure I shows the areas where traditional crime and computer crime overlap, as well as areas in which computer crime represents new criminological phenomena.

Crime theories and computer crime

Traditional crime theories linking crime to environment, economic need, conflict and cultural conflict, and biological makeup, are generally motivation theories. Perhaps opportunity structure theories are more appropriate when describing computer crime. In opportunity structure theory, the actual process of the crime can appear as the result of several factors: attitude toward moral norms and laws which do not deter this particular form of criminal activity, motive, subjective calculation (risk-taking), and circumstance (anonymity, low level of social

This is a summary of *Datorteknik och Brottslighet*. Swedish Crime Prevention Council, Atlasmuren 1, 2 tr, 113 21 Stockholm, Sweden. April 1985. 228 pages. (NCJ 100521)
Summary published June 1986.

control, lack of control structures, low risk of detection).

Particular factors influence the vulnerability to computer crime:

Complexity and volume of data

One of the most significant factors is the complexity and concentration of data in massive data systems. For instance, in Sweden, the National Insurance Administration's automatic data processing (ADP) system is used to collect, store, search, and retrieve data by all central and local offices, which are connected via a large telecommunications network. The integrated system allows access to the National Health Insurance system, the national assistance and subsidy system, the pension system, and statistical reporting systems. The files contain data on 1.7 million children receiving child subsidy and other payments; 0.2 million persons receiving income subsidies and public assistance; 6.6 million registered insured people; 1.9 million pensioners; 1.3 million children who are wards of the state; and 6.7 million persons contributing to the national pension fund. Approximately 92 million crowns are paid out yearly using the system.

Other systems containing massive amounts of data are within the centralized banking system (all banks in Sweden share an integrated system allowing transactions to be conducted by customers from any bank regardless of the bank in which they hold accounts), the police system, the motor vehicle administration, the tax administration, the post office, and the telephone company.

In terms of automation, the banking system may be the most complex. Numerous transactions take place electronically, including deposits, withdrawals, clearing between banks, intake of loan payments and other regular payments, currency exchange, accounting, and investing.

Distance from victim

Another vulnerable factor is distance. The perpetrator in traditional crime is usually face to face with the victim. In computer crime, the geographical distance between the offender and the involved system can be considerable. Even national borders are not a factor.

System error

A third vulnerable factor is the likelihood of computer error inherent in computer systems. The frequency of noncriminally-induced computer error helps hide criminal activity. Most of this error stems from poor data quality, but in an automated environment, poor data quality is often difficult to detect and correct. In normal textual information, a typographical error, for instance, is easy to correct. However, computer data often are made up of codes for which the correct code is difficult to detect and track. Computer error can result from a number of sources—design and use errors, entry or transaction errors, interpretive error, hardware error, and software error. Baily (1983) estimates about 35 percent of computer failings due to human error, 20 percent to design error, and 30 percent to poor instruction, documentation, training, and other workplace environmental factors.

Anonymity

Another facilitating factor in computer crime is the anonymity of the work environment within which persons can pursue crime. This anonymity has increased with the introduction of terminal systems and data communication. The various parties who can touch a particular transaction "disappear" in an automated environment. In a manual environment, physical evidence (the money, paper documentation, witnesses to the incident) exists, and a physical exchange of the stolen item usually takes place. In addition, the perpetrator has a particular ingrained attitude toward the paper money or goods (which might provoke guilt), whereas in computer crime tangible evidence usually is lacking.

Time

A final opportunity factor is time. The process involved in carrying out traditional crime can take minutes or hours; in computer crime, the process might take seconds or parts of seconds. The traditional criminal might calculate this passage of time (during which he is at high risk for discovery) as a risk factor. In computer crime, this risk factor is greatly reduced.

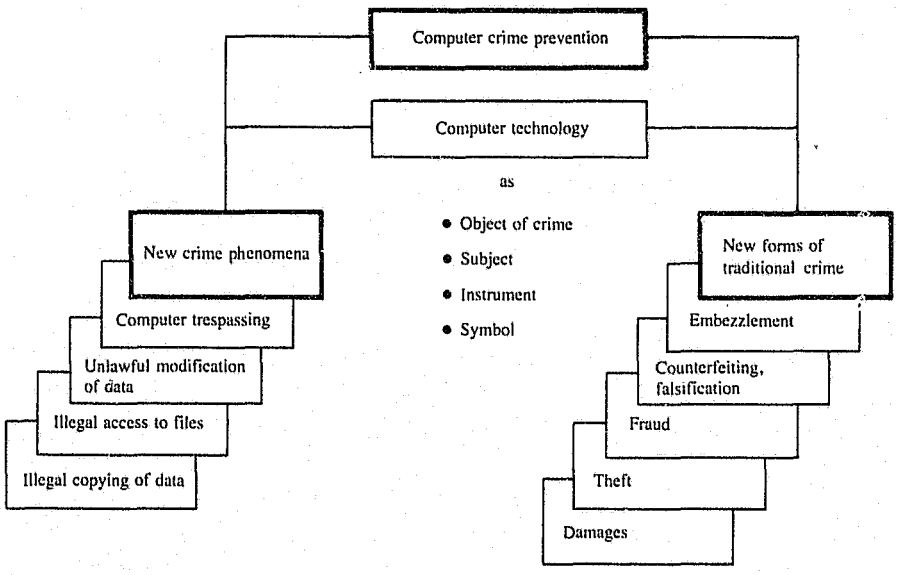
Empirical studies

Because so little empirical data on computer crime exist, two empirical analyses were conducted to identify variables common to computer-related crime. The studies were difficult to conduct because of the lack of data, the lack of a clear and generally accepted definition of computer crime, the difficulties in detecting computer crime, and the low incidence of reporting these crimes, as well as the likelihood that they may be reported under other crime categories. The results of the studies should be considered in light of these difficulties and in light of the criteria used in the studies; only crimes involving embezzlement and theft of computer equipment were considered.

First study—embezzlement and its methods

Official efforts to gather data on computer crime began in Sweden in 1977 and were

Figure 1



retrospective to 1967. For the period 1967 to 1977, a total of only 30 cases is recorded; for the period 1977 to 1983, a total of 33. To supplement this small number of records, the first study involved the analysis of all crimes occurring within selected crime categories for the period 1981 to 1983 to identify all crimes of grave embezzlement (351); analysis of all cases of computer-related grave embezzlement, breach of trust, or both, occurring during the period 1981 to 1983; analysis of 10 cases involving serious embezzlement occurring from 1979 to 1980; analysis of a 10-percent sample (150) of cases of serious fraudulent crimes occurring during 1983 (no instances of computer-related sample); and collection and analysis of crimes registered with authorities other than the criminal justice system during the period 1974 to 1983.

The study cases were divided into two categories: those cases involving computers (ADP group, 48 cases), and those not involving computers (non-ADP, 180 cases). An analysis of court records, police investigation reports, and criminal histories yielded a list of 29 variables that were coded and classified. The variables were used to compare and describe computer-related crime and traditional crime, the perpetrators, the situations within which they operated, and their mode of conducting the crime.

The chi-square method was used to distinguish the ADP from the non-ADP group in terms of frequency of the variables, and an expression was constructed that approximately followed the probable distribution known as X^2 distribution. The hypothesis of difference between the frequency of variables was tested to a 5-percent level.

First study results

Analysis of results showed that banks and post offices (in Sweden, post offices act as banks for simple routine operations like deposits, withdrawals, and bill paying) were the most likely targets of crimes by the ADP group (79 percent of crimes), but were one of the least likely targets for the non-ADP group (5 percent).

A logical correlation was found between the number of crimes committed per person and the duration of the person's offending. In the 48 cases of people in the ADP group, the total number of crimes was 1,062, or 22 crimes per case. The duration over which the crimes occurred and remained undetected was significant. For the non-ADP group, 54 percent of crimes were detected within 1 year; for the ADP group the corresponding figure was 39 percent. Forty-seven percent of the non-ADP group and 60 percent of the ADP group had committed their crimes over a period of 1 to 9 years without detection. The average amount of money embezzled was higher for the ADP group (200,000 crowns) than for the non-ADP group (140,000 crowns).

Additional findings were that:

- More females were involved in the ADP crimes than were involved in the non-ADP crimes (44 percent compared to 13 percent) even though men were still the predominate offenders.
- Offenders in the ADP group did not necessarily have a high level of education or training in computers; rather they had a practical knowledge of routine functioning of the systems.
- ADP offenders were slightly (not significantly) more likely than non-ADP offenders to be married and have families.
- ADP offenders were more likely than non-ADP offenders to have mid- or low-level jobs, but were likely to have been employed longer at the company from which they embezzled.
- Although drug/alcohol abuse information was not available on all persons, the percentages of incidence for persons on which information was available was similar for both the ADP and non-ADP groups (14 and 15 percent, respectively).
- Offenders in the ADP group were significantly younger than those in the non-ADP group (71 percent under 40 years of age as compared to 42 percent).
- Information on motive had to be derived from case records, coded, and analyzed. Results indicate that economic motives were probably more likely to explain the behavior of the ADP group (68 percent) than the non-ADP group (34 percent).
- Offenders in both groups were unlikely to have had previous criminal histories.
- Although various types of crimes were apparent in the 48 ADP cases (rolling loans, transfers between accounts, delayed or fictitious deposits in connection with rolling loans, corrective manipulations, manipulations with internal accounts, deliberate overdrafts, spatial transfers and bogus deliveries, and manipulation of access codes), the overwhelming majority of cases involved manipulations of input data—transfer and transaction techniques, particularly simple transfers into one's own or another's account, rolling transfers, or corrective manipulations within internal accounts or in accounts in which data were transmitted from another company.

Second study—computer equipment theft

Besides the embezzlement study, an additional small study looked at the 59 cases of computer equipment theft reported to the Goteborg police between 1980 and 1984. Analysis of the data showed the following:

- The incidence of computer theft appeared to be increasing (80 percent of the crimes occurred in the last 2 years).
- Most crimes involved money values of between 1,000 and 5,000 crowns.
- Theft usually involved computer hardware, such as the computer itself, or modems, monitors, etc.
- Most often, the goods were stolen from the owner's automobile (37 percent), from a business (15 percent), or a shop (15 percent). Least often were they stolen from homes (3 percent).
- Break-ins were associated with only 18 percent of the thefts.

Second study results

Information on these cases was not sufficient to derive results on modus operandi or motive.

Prevention

The purpose of the studies was to identify areas of vulnerability in an automated environment so that suggestions for more effective control systems could be developed. The results show that a number of the computer-related crimes could have been avoided or discovered earlier if the injured party had known about similar computer crime in other organizations. This applies mainly to banking and postal services, which have similar transactions.

The great majority of cases involved manipulating input data. A logical safeguard is verification of basic documents and primary data, one of the weak links in the system of surveillance. Logging routines automatically registering the transactions do not appear to be an adequate substitute for quality control of primary data.

Controls also are needed for checking computer errors. While comprehensive investigation into the origin of every error may not be economically feasible, systems can be designed to automatically

feed erroneous and modified transactions into a temporary file where staff can examine these later.

For online systems, quick detection and correction of errors is particularly important. Better control routines for handling and verifying errors are also needed (including typographical errors and transactions). These routines should be well documented, closely adhered to, and systematically enforced. Regular statements to customers can help to protect accounts from tampering.

Several of the crimes involved internal accounts in which unlawful transactions could be performed easily. "Dormant" accounts were particularly vulnerable to unlawful activity. A system of control adapted to the new technology and to protect dormant accounts would be important.

There are groups of clients who for various reasons do not observe and check all transactions; e.g., persons with several accounts and numerous transactions, or elderly persons. Supplementary methods of control are needed for these accounts. Access control impedes outsiders but appeared to be ineffective in hindering persons who are inside the organization or who have knowledge of the system. Future access controls should take this into account.

Most computer criminals have been employed in the organizations for several years and have no indicative history of problem behavior. They are not highly specialized but tend to be terminal operators with insight into the system. Personnel selection strategies and surveillance of data processing specialists are therefore no safeguard against computer crime.

Overall, the study results point to the need to reduce vulnerability by changing the amount of opportunity to access the system illegally. This is particularly critical since the trend in computer technology is toward putting nearly every employee in front of a terminal. Figure 2 illustrates the various areas in a system that are vulnerable to crime and for which controls are needed.

New technology

New technology can facilitate crime prevention. For instance, banking machines are becoming common. With these machines, bank customers in any location can use their cards to access a central data bank that identifies their cards and the banks in which the accounts are held. The customer is then linked electronically to that account and a transaction can occur. The lack of a middleman to rekey data will reduce the likelihood of keying error.

In addition, credit cards are becoming more sophisticated. Newer versions include an identification number along with the credit card account number. The most sophisticated is a card with its own memory and processor. The memory can hold many bits of data on the person (e.g., person number, driver's license number, other identification numbers, address) as well as process information for banking transactions. It allows the customer greater security, permits its use anywhere, ensures payment to the store where the customer shops, and eliminates interference in the process of electronic funds transfer, since machine debiting from the customer's account would be accompanied by immediate machine crediting to the store account.

Other technological safeguards, such as cryptographically coded check digits, can be used to spot errors or changes to data in a file.

Implications for the future

The future will no doubt see an even greater trend toward automation. In the banking industry, for example, a new generation of systems will include card readers, keyboards, and screens, so that customers' identification numbers must be used for transactions to take place. Self-service banks, in which customers would conduct most banking transactions, check and reconcile their accounts on a monitor, and pay bills without the aid of a middleman, will become the norm. Home banking and datavision are undergoing experiment; in these, persons and companies are able to conduct routine banking transactions, check their accounts, and keep their books from a terminal in the home or office. In addition, international data networks are being created so that money can be electronically transferred to banks in other countries.

Sweden must prepare itself for this future of automation. Not only must a definition of computer crime be developed, but the legal community must acknowledge the great range of possible criminal behavior involving computers. This realization should cause a full-scale examination and possible redirection of the penal code, now directed toward describing and punishing traditional crime.

Figure 2