Computer crimes and countermeasures

Introduction

It is impossible to imagine a world without computers. Every aspect of our existence in the physical realm is in one way or another influenced by computer technology. From household budgets to outer space programme, medical science to high-tech war, there is a dependence upon the capabilities of computers that have revolutionised our existence. The banking system with EFT (electronic fund transfers) over international borders is moving billions of dollars amongst banks and businesses today. Unfortunately, with the computer age came computer-related crimes.

The possibilities to defraud institutions with millions have in fact become easier through computer than with manual operations.

Managers and security experts today are confronted with the problem of protecting their companies against computer crimes while they themselves may not be computer literate. This, however, does not exonerate them from a responsibility which many today are treating with little sincerity, if any at all.

Computer vulnerability

A computer with all its romantic glamour for lay people and intellectual challenge to experts and amateurs is firstly a physical object and therefore subject to destruction and abuse.

Computer crime and abuse generally fall within the classification of fraud, disclosure, modification, destruction or denial of service (sabotage or destruction). A study by the Patton Accounting Center at the University of Michigan revealed the following fears of chief executive officers and other senior managers. The potential disasters they feared most were:

- business interruptions;
- destruction of accounting systems and control records;

G T du Preez  DPhil(Sos)(Cape Town)
Institute for Criminology
University of South Africa

C J Roelofse  MA(Unisa)
Security Consultant
Theliop Loss Control International
Randburg

Opsomming

Rekenaars het 'n revolusionêre invloed op ons samelewing. Daar is geen gebied waar hierdie tegnologie nie 'n invloed het nie, van 'n algemene huisbegroting tot op die gebied van gesofistikeerde oorlovoering is die veranderinge enorm.

Ongelukkig het misdaad ook in hierdie area van ons samelewing skrikwekkende afmetings aangeneem, terwyl die potensiaal vir grootse kaal vrillende fenomenaal is. Tipiese misdaad is bedrog en verduistering, spioenasi en sabotasie en saakbeskadiging is. Tog het dié tegnologie juis 'n soort romanse en uitdaging aan misdadiigers gebied om die rekenaar te probeer uitoort. 'n Tipiese voorbeeld hiervan is rekenaarvirusse.

Daar is egter geen rede tot kommer nie, mits die voorkomingsmaatreëls wat beskikbaar is nougeset toegepas word. Daar is egter aspekte soos die bepaling van verantwoordelikheid, wetgewing en opleiding wat dringende aandag verg.
• manipulation of accounting and control records to cover or affect irregularities; and
• exposure of sensitive information.

They also feared a loss of competitive edge due to

• obsolete equipment, and
• excessive expenditures for information systems (Kluepfel 1989:73).

Although this survey shows a fear of computer-related crimes and abuse, managers in general seem to have an almost voluntary ignorance of computer protection and security. There is a need for greater management awareness and involvement in protection programs. It is amazing that whilst living in the computer age many managers and security specialists know very little about the systems that influence their lives and businesses so drastically. Computers are vulnerable and there is a need to identify the risks and implement sound countermeasures.

**Physical destruction**

Attacks on computer centres occur quite often with sabotage, fire and physical attacks (e.g. shooting) being the most common forms. The following are examples of such attacks:

• **July 1978**: Seven armed terrorists attacked a computer centre in Turin by setting it on fire with Molotov cocktails.

• **On 20 May 1980** a French activist group calling themselves the Committee on the Liquidation or Deterrence of Computers (CLODO) and a terrorist group Action Directe claimed responsibility for the destruction of computer systems and data during an attack on Philips Data Systems.

• **June 1980**: Terrorists ransacked a hall in Toulouse that had been prepared for an international symposium. They left a message ‘Scientist swine. “NO” to capitalist data processing’.

• **March 1981**: An IBM computer of the Banque Populaire in Toulouse has been damaged (Campbell 1988:57–59).

According to two physical security experts, ‘Similar incidents abound. In the last decade at least 57 computer centres in Europe, including six bank computer centers have been attacked by terrorists’ (El-Baghdadi & Singh 1989:63). Physical destruction of computers is a very effective way for terrorists and vandalists to achieve their objectives but it is also the most risky type of operation exposing them to security reaction and identification e.g. by video or physical description. Far more menacing are those crimes which are hidden to human observation. The two most menacing crimes in this field are fraud and virus introduction.

**Fraud**

Computer fraud is normally committed in three ways:

**Input fraud**

As suggested by the terminology used, fraud is committed by manipulating data being fed into the computer. A very common application is to transfer funds to a personal account (Du Preez 1991:307). In America the average bank robbery nets around $20 000 while the average crime involving electronic funds transfer (EFT) nets somewhere around $500 000 (Jackson 1984:153). According to the same author the average electronic theft takes about 3/1 000’s of a second!

**Program manipulation**

Considerable skills and access to relevant programs are necessary to commit this crime. One of the most common methods used is the ‘negative rounding off method’ whereby final amounts of, for example, salary cheques are rounded off to the nearest figure. Sums of money accumulated in this way are then deposited in the personal accounts of criminals.

**Output manipulation**

The third method entails theft of computer-printed cheques, copies of software, etc. Another method of output manipulation could involve the destruction of delivery notes, which serve as original documentation for invoicing. Theft of cheques by this method seems to be the most common crime (Du Preez 1991:307).

**Viruses**

Computer viruses are the latest addition to computer vulnerability. Although much has been written and said about this computer ‘disease’ it is not as new as the recent interest shown in it. Viruses were exposed on 3 November 1988 when a graduate of Cornell University launched a malicious computer program into a major national computer network. The virus attacked 6 000 computers that were linked to the network. A total damage of $100 million occurred (Yovel 1990:65). Although this event enjoyed widespread coverage in the media it was actually a new awareness of an old problem. The first virus – though not called that – rightfully belonged to John von Neumann. He presented a paper already in 1948 on the mathematical concepts of a self-replicating code. His experiments with the self-replicating code were the forerunners of viruses and defined the way by which viruses spread.

A computer virus can be defined as a programming code developed with the specific intent to replicate itself over and over into other programs. It replicates itself in such a manner that it actually becomes part of
the infected program: The virus lies dormant but is activated every time the program is running. Viruses are pieces of programs that infect other programs. Viruses attach to data, thereby destroying the integrity thereof. The virus stops in the data and cannot spread further unless the data becomes a program. Therefore computers that only pass data between separate systems cannot perpetuate the virus (Slayden 1989:110).

As a natural virus is target specific, a computer virus is also target specific. This means that in nearly every case there must be specific knowledge about the target to develop the virus. Unfortunately the vast occurrence of standardisation in personal computers software is actually instrumental in making viruses infectious.

Computer viruses fall into three basic attack styles.

**Boot infectors**

The initial loading sequence that allows computers to function typically starts executing instructions at a predefined location. The instructions following this predefined location are the administrative and technical operations necessary to allow user interface with the system.

Boot infector programs according to Slayden (1989:111) embed themselves in these bootstrap instruction sequence and capture the operation. The virus code replaces the original bootstrap code in its permanent memory. The boot infector always remains in control infecting any other system that comes into contact with it.

**System infectors**

These types of viruses attach themselves to system files required for the day to day normal functioning of the computer. They remain dormant until a specific event occurs and is then activated and start affecting the system.

**Utility and program infectors**

These are the most common but also the most dangerous viruses. The virus can be spread by any program to basically any other program. The virus spreads in one of two ways:

- The virus copies itself to every other program in the computer. Every time the infected program is run the virus gains control.
- Once executed the virus remains resident and infects each program used after the virus is in control.

By nature computer viruses can be responsible for serious problems in computer systems. Not only can it reduce computer space and slow down programs, but it can distort, change and destroy data very quickly. Viruses introduced into systems can be the source of blackmailing and even if money is paid to the black-mailers the victim has no assurance that the virus will be withdrawn.

**Hacking**

Hacking simply means to gain unauthorised access into a computer system via a modem or landline meaning that the hacker can perform operations on the system and gain access to data. The real threat is the criminal who can use the technology to embezzle, trade on inside information, puff the price of stock access of competitors' data, transfer millions of dollars electronically and electronically impersonate other users of the computer network (Kluepfel 1989:75).

Although figures for the RSA is not available the annual loss through industrial espionage in the USA is estimated at $1 billion (Weiss 1991:44).

During the preceding discussion some of the main problems in computer-related crimes were discussed. In security it is essential to now venture into protection against such acts in order to obtain the greatest possible preventive advantage in our fight against crime.

**Physical security countermeasures**

Physical security measures are required to protect computers and their related systems (PC security is not included in this article). The main object being denying physical access to computer components. The risks of sabotage and destruction can largely be prevented through physical barriers, access control, alarm systems and fire-detection and fire-fighting equipment.

Physical protection of computers also means creating an environment which is free of water, dust, overheating and static electricity. This indicates original design inputs in building construction in order to protect computers effectively. The following aspects of physical security are important:

**Site selection**

A mainframe system, especially of a computer bureau, must be well protected. Part of the problem can be solved by selecting a site in quiet suburbia away from the mainstream day-to-day city life. Future developments of the area should be considered particularly:

- mining rights
- overhead powerlines
- educational institutions
- sports facilities
- highways and secondary roads construction.

The location of the computer mainframe in the
building is equally important. The following principles should be borne in mind:

- Waterpipes should not pass directly over the computer room nor under its suspended floor.
- It should not have windows opening directly to the outside.
- Fire escapes should be alarmed and monitored by closed-circuit television (CCTV).
- Blast-resistant and watertight walls, roofs and ceilings should be standard.
- Fire-fighting systems such as halom should be automated with handheld backup units.
- External as well as internal alarm systems and proper access control systems such as explosive and metal detection should be provided.
- A temperature tolerance alarm should be installed.
- A proper dustproof air conditioning system is essential.
- Emergency power supplies with uninterrupted power supply (UPS) and battery backup for the system and emergency lighting are standard features.
- Fireproof ducts, cable protection and backup storage facilities round off the essentials of physical security.

In existing buildings it may be difficult to backfit systems, change water-pipes, etc, but it is well worth the effort and money to upgrade physical security as far as possible. As a final hint all computer rooms should have large enough plastic sheets to cover machines in the event of water leaks.

**Personnel subsystems countermeasures**

These countermeasures are aimed at the proper identification of users to prevent unauthorised access into the system.

Passwords have been the main component of user identification in the past almost thirty years. However, a single identification system is not adequate to proof user identification. The many problems associated with passwords – the necessity of frequent password changes, the irrepressible habits of users who write them down, the vulnerability to statistical attacks and guessing, the ease of casual interception in networks and the hassles of password administration – are industry lore, but the password remains the bedrock. It is the first and basic level of user authentication. Passwords, however, represent only one of three basic ID authentication methods. These three methods are

- something one knows – a memorised secret code, phrase, number or fact known only to an individual user and his or her computer;
- something one possesses – a discrete token that strongly resists counterfeiting such as a signet ring key, credit card or badge; and
- something one is – a measurable personal characteristic, such as a fingerprint, signature, retinal pattern or voice print.

Basically all authorities today agree that a combination of at least two, independent ID authentication systems should be used.

Two-factor authentication is necessary to ensure accountability, deter insider abuse effectively and withstand legal scrutiny necessary for successful prosecution of offenders. An example of two-factor ID authentication can be found in automatic teller machine (ATM) cards. To use a card a depositor must first insert it into a card reader at the ATM terminal, which reads data stored in the card’s magnetic stripe. The terminal then demands a second identifier, the user’s memorised password or personal identification number (Weiss 1991:44–45). In high-risk institutions it would be advisable to use a two-factor system with a password and personal characteristics, preferably fingerprinting, as a possible combination. The use of a second independent identifier vastly increases the certainty of end-user authentication. Managers need no longer worry about one co-worker learning another’s password, outsider and hacker related threats virtually disappear and internal threats always more prevalent and serious are controlled because audit trails finally offer solid accountability (Weiss 1991:45).

**Cryptography**

Most computer-related fraud is committed by insiders, people who have legitimate access to and knowledge of the system. Thus a security system should be designed to provide protection against the inside attack. A properly constructed cryptographic security system can provide effective protection. Encryption is the basis of all crypto systems. It converts the data to an unintelligible form called a cipher. Recovering the data from the cipher is called decryption or deciphering. The encryption and decryption processes are usually accomplished by means of a complex mathematical algorithm controlled by a key (Avarne 1988:39).

Encryption in itself is not sufficient to ensure the integrity of a message. Message authentication is a technique applied to ensure that data cannot be altered without detection. A message authentication code (MAC) or a cryptographic check sum is appended to each message. The value of the MAC is determined by the contents of the part of the message needing protection. In figure 1 the encryption-to-decryption process is explained.

![Figure 1](image-url)

**Figure 1**

- Plain text
- Key
- Encrypt
- Ciphertext key
- Decrypt y
- Plain text

(Avarne 1988:41)
From figure 1 it can be seen that a plain text (legible) message is encrypted by using a key. Data is then transmitted in ciphertext and is again decrypted by using a key. The protection afforded by a cryptographic process is no greater than the protection given to the key controlling the process. Key management is generally concerned with the following:

- **Key generation.** Keys (in algorithm) must be generated in a random and unpredictable manner.
- **Key distribution.** When using a conventional cipher, parties who wish to communicate must share a common key which must be distributed securely (Avarne 1988:41). A manual distribution system commonly applies the split key system. Parts of the key are separately distributed. A perpetrator of a malicious act can only decipher the message if he obtains all parts of the key.
- **Key hierarchy.** A key hierarchy normally denotes a system whereby keys at one level in the hierarchy can only operate on keys in one level down.
- **Key storage.** The usual application is to permit keys to assist in plaintext form only within a separate, tamper-resistant security module. A special encrypting key called a local master key (LMK) and known only by the security module is used to encrypt keys while they are stored outside the module.
- **Key change.** To avoid any successful cryptanalytic attack or to limit the impact of a successful breach of the system keys should be changed regularly. The more sensitive the data being transmitted the more regularly keys should be changed.
- **Key deletion.** Procedures are also required to ensure that plaintext keys such as those used during manual distribution, are destroyed when no longer required (Avarne 1988:42).
- **Key configuration.** The length of the key is a critical factor in key configuration. The shorter the key the more likely it is to break the cipher. A minimum of eight characters and numbers in random pattern provides a good level of security.

**Methods to prevent breaking of codes**

To prevent someone from breaking a code users should:

- choose a strong encryption cipher;
- change the key often;
- segment messages;
- send nonsense messages in between some of the real ones;
- encrypt the data during storage and transmission;
- administer regular security checks on employees;
- properly destroy discarded data (media ribbons, discs, printouts);
- encrypt or erase hard drives if they are sent for service;
- keep unencrypted backup locked in a safe place in case the data is damaged on the disc or contaminated during transmission;
- keep a personnel policy on file that notes key and password handling;
- disable all default and utility passwords and accounts;
- make sure security is handled and checked by more than one person;
- make sure keys or passwords are stored in an encrypted form; and
- synchronize data transmission times to track whether data is rerouted or slowed by a tap (Kesim 1988:47).

By encrypting data both insider and outsider interference can be limited. Hackers will find it extremely difficult if not impossible to break a properly developed and controlled security system.

**Virus countermeasures**

Viruses can be introduced from outside or from within. Kluepfel (1989:11–112) suggests some very useful countermeasures. The fact must be stressed that it is not one single countermeasure that provides protection but an arrangement of integrated controls and procedures. The following can be done:

- Treat public domain and shareware software with care.
- Do not use software from bulletin boards or electronic mail.
- Do not connect to a WAN (wide area network).
- Use password-protected computer dial-up telephones to reduce the possibility of an unauthorised user source of contamination.
- Never boot from any floppy disk other than the original write protected diskette from the original distribution package.
- Watch for changes in the pattern of the system’s activities or responses. Immediately investigate anything that has not happened before.
- Write protect all boot floppies.
- Remove floppies from drive slots and store them in filing cases when they are not being referenced.
- Isolate new software until it is tested thoroughly.
- Before loading new software make a complete backup and store it in a safe place.
- Do not connect dial-ups to the system without using thoroughly trusted procedures.
- Use software programs that identify and prevent viruses from infecting or destroying data. Unfortunately no one software will cure all viruses.

**Legal protection**

The term computer crime is actually just a buzzword because the crimes committed such as fraud and
embezzlement, theft, malicious damage to property, are common law crimes. Under private law it is possible to institute proceedings to recover losses introduced through malicious acts. In the United States various pieces of legislation such as the Computer Fraud and Abuse Act of 1986, Computer Security Act of 1987 and the Computer Virus Eradication Act of 1988 were passed making computer-related crimes specific statutory offences. In South Africa no such laws exist and it would be useful for legislators to consider a comprehensive Computer Security Bill combining all the various aspects of computer crimes on security requirements into one act for South African circumstances and needs. However as Senator Patrick Leahy pointed out, 'We can pass laws that make criminal penalties for unauthorised access to computers, but we also need improvements to increase security. It is a sad truth of modern life that laws against burglary will never safeguard a home like good locks' (El-Baghdadi & Singh 1989:66).

Responsibilities

Like with most other issues in society, awareness of it is half of the solution. Many times computer security is the responsibility of a line functionary with no security knowledge or a security functionary with no computer experience. Both of these applications can lead to disaster. There is no doubt in the minds of the authors that the responsibility for computer security rests squarely on the shoulders of management. They have one major problem though – TIME.

Conclusion

In such a complex matter as computer crimes and prevention, an article such as this can never hope to provide answers to all problems. It is hoped that it would however create an awareness of a need to come to grips with a very essential part of our society and business world in order to minimize crime in this vital application of technology.

Bibliography