Can computer security really make a difference?

Craig S. Hannaford

How classic computer security principles could have prevented computer crimes

Much has been written in the popular press about the onslaught of the information age and the construction of the information superhighway. We are regularly warned of the dangers that these technological advances will bring to persons concerned with the integrity of computer systems. A recent Organization for Economic Co-operation and Development report on the Security of Information Systems commented on this threat and the need for proper computer security:

> Explosive growth in use of information systems for all manner of applications in all parts of life has made provision of proper security essential[1].

Indeed, information technology (IT) has exploded and, in many cases, the provision of proper IT security has taken a back seat to the expedient implementation of new technologies. It often seems that local area networks (LANs), computer communications networks and other forms of computer technology are implemented without a real analysis of the security implications involved.

This article will provide some of the typical computer crimes that police and other investigative agencies have encountered. Also, some basic IT security principles will be outlined. The article will then discuss some recent computer crime cases and examine these incidents in the context of IT security principles. In each case, the application of a sound IT security programme could have prevented the crime from occurring in the first place.

What is computer crime?

Many countries have laws that deal specifically with computer crime. The Council of Europe addressed the issue of computer crime in its recommendation R (89) 9. This recommendation provided a minimum list of computer crime laws, which all countries should enact. This list, although not exhaustive, outlines the types of computer crime that can occur:

- *Computer-related fraud:* the input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing, that influences the result of data processing, thereby causing economic or possessory loss of another person with the intent of procuring an unlawful economic gain for himself or another person.
- *Computer forgery:* the input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing in a manner or under such conditions as prescribed by national law, that it would constitute the offence of forgery if it had been committed with respect to a traditional object of such an offence.
- *Damage to computer data or programs:* the input, alteration, erasure or suppression of computer data or computer programs, or interference with computer systems, with the intent to hinder the functioning of a computer or a telecommunication system.
- *Unauthorized access:* the access without right to a computer system or network by infringing security measures.
- *Unauthorized interception:* the interception, made without right by technical means, of communications to, from and within a computer system or network.
- *Unauthorized reproduction of a protected computer program:* the reproduction, distribution or communication to the public without right of a computer program, which is protected by law.
- *Unauthorized reproduction of a topography:* the reproduction without right of a topography, protected by law, of a semi-conductor product, or the commercial exploitation of the importation for that purpose, done without right, of a topography or of a semi-conductor product, manufactured by using the topography[2].

Managerial Auditing Journal, Vol. 10 No. 5, 1995, pp. 10-15 © MCB University Press Limited, 0268-6902

Computer law in Canada

The Canadian approach to computer law has been to provide for specific sections in the Canadian Criminal Code[3] relating to computer offences. Section 342.1 (1) of the Criminal Code reads:

> Every one who, fraudulently and without colour of right,
>
> (a) obtains, directly or indirectly, any computer service, (b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system, or (c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offense under section 430 in relation to data or a computer system,
>
> is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction[3, p. 495].

Section 342.1 (1) of the Criminal Code is often used to prosecute computer hackers who have broken into computer systems. In Canada, this section has been used to prosecute persons who were former employees of a company and who remotely logged on to a company computer after they had been terminated. This section has also been used to prosecute persons who have tampered with phone-switching systems and voice mail systems. Section 430 (1.1) of the Criminal Code states:

> Every one commits mischief who wilfully
>
> (a) destroys or alters data;
> (b) renders data meaningless, useless or ineffective;
> (c) obstructs, interrupts or interferes with the lawful use of data; or
> (d) obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto[3, p. 578].

The penalty provision for Section 430 (1.1) Criminal Code is similar to that of Section 342.1 Criminal Code.

The mischief to data section could be used in cases such as a former employee who encrypts important working files prior to being terminated. Another example could be where an employee performs a low level format of his computer's hard disk prior to being terminated, thus destroying important company information.

There is one other section of the Canadian Criminal Code that is used in computer crime cases. Section 326 of the Criminal Code reads:

> Every one commits theft who fraudulently, maliciously, or without colour of right, uses any telecommunication facility or obtains any telecommunication service[3, p. 480].

It is common for computer hackers to loop their phone calls through phone systems of unsuspecting corporations or government agencies. This can result in large amounts of fraudulent telecommunications usage with the corresponding economic loss to the victim organization.

One other area of computer crime that has grown quite dramatically over the last few years is the copying and selling of commercial software. In Canada, the Copyright Act prohibits this activity and fines as high as $1,000,000 or five years' imprisonment can be imposed[4].

Overview of information security principles

The basic elements of information security principles are widely known. However, it will be useful to review these principles briefly so that they can be readily referred to during the discussion of various computer crimes that have occurred.

Information technology security is composed of seven necessary components:

(1) *Administrative and organizational security.* This component involves the development of an overall IT security policy and the implementation of that policy. Some of the functions associated with this component are identification of risks, definition and assignment of individual security duties, designation of restricted areas, development of authorization procedures, recognition of external and contractual dependencies and development of contingency plans.

(2) *Personnel security.* This component includes the detailing of security requirements for each job function, ensuring that job holders meet those security requirements, providing adequate security training, providing sufficient access control to system resources through appropriate personnel identification methods. Another important part of personnel security is attention to hiring and termination of employees.

(3) *Physical and environmental security.* IT systems should be given adequate protection from natural and man-made hazards consistent with the importance and sensitivity of the IT assets being protected. Factors to be considered include site planning, control of access to restricted areas, protection against physical damage, protection against power and environmental failures, and safeguarding of IT materials and supplies (including waste disposal). For example, it is well known in the computer investigative community that computer hackers have obtained valuable information such as employee lists and account numbers from searching through refuse containers. One recent incident that underscores the importance of this type of IT security was the bombing of the World Trade Centre in New York. One can speculate that those companies who had adequate physical and environmental security programmes were able to endure the disruption that this terrorist act caused to their IT assets.

Other companies were probably not so well prepared.

(4) *Hardware security*. This component deals with security features that have been built into the computer hardware itself and also any support and control procedures required to ensure the effectiveness of those features. Hardware security features can address the areas of identification, isolation, access control, surveillance and response techniques. Some examples of these features are terminal answer back systems, magnetic cards and badges, write rings on magnetic tapes, security consoles and alarms, maintenance logs and examination of new equipment for viruses.

(5) *Communications security*. Many computer systems in use today involve the use of some sort of communication line, whether it be in the form of network cabling or the use of telephone lines. Risks such as mis-routeing of information, cross-talk between lines or wiretapping must be considered. Proper siting, the use of redundant systems and electronic screening procedures are some steps that can be taken to reduce these risks.

(6) *Software security*. Many security functions can be performed by software. Software security features can address some of the same security concerns as hardware security. Software security systems should be able to differentiate between the various entities subject to security measures in a system. Examples of such procedures include passwords, account numbers, volume labels, tape numbers, access lists and logging of usage.

(7) *Operations security*. This component of IT security ensures that proper policies and procedures are in place so that IT capacity is available when needed and that any security risks inherent to a particular system are acceptable. The key part of this component is to ensure that duties and responsibilities are clearly assigned and that separation of duties has taken place.

Operational activities can affect many significant areas within an organization. For example, operations areas should have procedures dealing with the storage, use, erasure and disposal of computer media. Cautionary procedures must also be in place to protect special forms and cheques. Controlling access to the computer operations room often falls into this category of IT security[5, pp. 3ff.].

This overview of IT security principles is by no means exhaustive. However, it provides a basic understanding of some of the areas to consider when implementing an IT security policy. In many cases, the lack of such policies has made it easier for a computer criminal to carry out his crimes. Let us now examine some of these crimes and determine what security features were lacking that allowed the crime to occur in the first place.

Computer crime case histories

These case descriptions are actual computer crimes which have been investigated by the Royal Canadian Mounted Police or by other Canadian police agencies. The cases are described in a generic manner as the IT security principles behind the cases are of concern and not the specifics of each case. Each case discussed is the subject of a police operational file and, in many cases, prosecutions have begun or are complete.

Case 1

A large institution was developing a new payroll system. The institution hired a computer consultant to program part of the payroll system. This consultant was allowed remote access to the institutions mainframe computer and was also allowed as much computing time as he needed. In addition, the consultant was provided with as much disk space as he required. The consultant was not, however, allowed to access any area of the disk space he chose. Eventually, the institution terminated the consultant's contract. The consultant had a serious problem in that he had spent considerable time developing a payroll program; however, in so doing, he had used several computer routines developed and owned by the institution. He needed those routines to obtain a working copy of the payroll program. The consultant did not have sufficient privileges to copy the required routines from the disk space where they were stored.

In order to bypass the computer security features of the institution's computer and obtain copies of the programs he needed, the consultant modified a low level utility program that talked directly to the computer's operating system without working through the security software installed on the system. The consultant modified this utility program to include commands to copy all the files he needed to disk space where he had full access rights. For good measure, he copied the institution's payroll file including personal information on employees. His last step was to download all this information to his home computer via his modem link.

Personnel security and software security considerations could have prevented this particular incident from occurring. The institution could have cut off or severely restricted the consultant's access to their system once they knew his contract was to be terminated. Fortunately for investigators, the institution had utilized much of the significant logging capacity of its computer system. These logs provided evidence to obtain search warrants and ultimately helped support a charge under Section 342 of the Criminal Code of Canada. This logging capability

demonstrated that the institution had a strong operational security system in place.

To protect itself further, perhaps the institution should have encrypted the information that was taken by the consultant. This would have added a greater degree of security to their software assets.

Case 2

A youth was dismissed from a telemarketing firm. While at the firm, he had access to their computer system. The system was available to employees via a computer modem, should an employee not be working at the office. After being terminated, the youth dialled into the computer system. His account and password had not been de-activated. He then downloaded customer lists and other personal information including credit card numbers, expiry dates and addresses. This information was used by the youth and his friends to commit credit card fraud.

Once again, personnel security principles were not followed. On termination of the employee, his account should have been deleted from the system. Implementation of proper communications security principles, such as the use of a dial back modem, might have prevented this crime from occurring.

Case 3

Search warrants were executed at a chain of computer stores suspected of loading illegal copies of computer software on to computers that were subsequently sold to customers. Over 100 computer systems were seized by police. These systems had to be analysed by forensic examiners to determine whether illegal copies of the software were in fact resident on the hard disks of the computer. The presence of this illegal software was subsequently confirmed; however, this is not the remarkable aspect of this case. On several of the computer hard disks examined, computer viruses were found. These were computers that were boxed up, wrapped in plastic and ready for shipping to the unsuspecting customer. The last thing a new computer owner would think about is the possibility that his computer contained a computer virus when coming from his supplier. This was in fact the case and it is unknown how many such infected systems had been delivered to unsuspecting computer purchasers in the past.

This case demonstrates the importance of proper hardware security. All new computer disks and other vulnerable magnetic media should be scanned for the presence of computer viruses prior to the new equipment being placed into service[5, p. 10]. It cannot be assumed that a new piece of computer equipment is virus-free simply because it came out of a box from the supplier.

Case 4

A terminated employee used his unexpired computer access code and password to dial into the company's computer. Once in the system, the employee downloaded information useful to him in a possible civil law suit. After obtaining the information in which he was interested in, the suspect altered the user logs in an attempt to hide his tracks. This case shows the degree of sophistication of some users and the fact that user logs may not detect all unauthorized activity. Once again, personnel security principles were violated. This user should have had his access privileges revoked immediately on termination. Further, sensitive information of the type taken by the suspect perhaps should not be stored on a computer that is accessible from outside the office area. It may have been advisable to encrypt this important information as well.

Case 5

Computer hackers in another country attempted to access computer systems illegally in Montreal, Edmonton and Vancouver as well as in various other countries around the world. Investigation by the national police concerned revealed that these hackers severely compromised computer systems all over the world. The hackers accessed these computer systems using established computer communications links. Most systems attacked by these hackers were UNIX-based. The techniques used by these hackers included many of the standard hacking approaches including:

- Trying default passwords that are often initially installed when a computer is set up but are often not removed when no longer required.
- Trial and error trying of passwords. Programs were written to try common user accounts and passwords. Such programs are readily available through hacker computer bulletin board systems.
- Use of Trojan horse programs that logged user account names and passwords to hidden files for later retrieval.The password and user ID of unsuspecting users were being captured and held in an obscure file for later retrieval by the hacker.

This case demonstrates the importance of administration and organizational security, communications security and operations security. The computer hackers involved accessed computer systems all over the world. No doubt they tried many systems that they were unable to penetrate. Further, it is believed that institutions or corporations with a strong administrative and organizational security policy are less vulnerable to this type of computer attack. Strong computer security awareness programmes could alert employees to contact security officials if any suspicious activity on the computer is observed, such as new or unusual files, slow computer response time and unusual computer activity[5, p. 5]. Knowledge that a computer

hacker attack has taken place is of prime importance to computer security officials. This knowledge allows the proper defensive approach to be taken in order to eliminate the attacks.

In this case, at least one Canadian corporate victim of these computer hackers was completely unaware that attempts to compromise its computer system had been made. One component of communications security is the provision of a monitoring system to record all attempts to gain unauthorized access to the computer system. All unsuccessful log-on attempts should be recorded in this log and then security personnel should follow up with a regular audit of this log. Computer communications systems can be configured to cut off the communication line after a set number of unsuccessful log-on attempts[5, p. 11]. It is possible in this case that these types of security features may have alerted the computer systems managers as to the computer hacking activity taking place and enabled them to take the appropriate security action.

The effective use of operations security features could have prevented many of the computer security breaches in this case. Probably the most glaring deficiency in many of the compromised systems was the hacker ability to crack user ID codes and passwords using password-cracking programs. These programs try common passwords such as names or birth dates. In addition, some systems are installed with default passwords (for example, a default user ID might be the word "supervisor" with the same word as a password). User IDs and passwords should be difficult for password crackers to determine. Many computer systems randomly generate a password consisting of upper and lower case letters and numbers. This type of password is much more difficult for a password cracker to defeat given the larger number of password combinations that are available.

Conclusions

Computer crimes do occur and it is anticipated that the number of such crimes will grow over the ensuing years. Computer crimes involve complex technologies, sophisticated telecommunications networks and, often, these crimes transcend national boundaries. These complicating factors make detection and prosecution of these crimes extremely difficult for national police agencies. Therefore, proper crime prevention techniques are essential in order to combat this new and growing type of crime.

Police organizations have excellent crime prevention programmes when dealing with more traditional crimes such as housebreaking or shoplifting. The general public has been educated as to what these crimes are and how they can protect themselves from such criminal acts. People generally have good locks on their doors and windows and ensure that their houses and possessions are secured while unattended. In these cases, the police and society have come together to fight crime in a preventive manner.

The same must hold true for computer crimes. Computer users and systems managers must ensure that their computer systems are secured and that basic IT security principles are followed. Should a home owner who leaves his front door wide open receive much sympathy if his house is burgled? Most would say not. Should a computer systems operator receive any sympathy if his system is damaged when it is wide open to intruders with no computer security in place? Readers can draw their own conclusions.

IT security is crime prevention. Computer systems managers must ensure that they have proper crime prevention practices in place. This is the major way in which computer criminals can be thwarted and the integrity of the world's computer systems can be assured.

References

1. *Guidelines for the Security of Information Systems*, Organization for Economic Co-operation and Development, Paris, 1992, p. 2.
2. *Computers and Crime, Functionality and Evidence*, International Criminal Police Organization, Lyon, France, 1993, pp. 29 ff.
3. *Martin's Annual Criminal Code 1992*, Canada Law Book, Inc., Arrora, Ontario, 1991, p. 495.
4. Canadian Copyright Act, Section 42(1).
5. *A Security Guide for the Electronic Office*, Royal Canadian Mounted Police, Electronic Data Processing Security Branch, Ottawa, Ontario, 1992, pp. 3 ff.
6. Meyer, G.R., "The social organization of the computer underground", *Computer Security Journal*, Vol. VII No. 1, p. 75.
7. Madron, T.W., *Enterprise-wide Computing, How to Implement and Manage LANs*, John Wiley & Sons, Toronto, 1991, p. 343.
8. Ainsbury, R.D., *Using Your Hard Disk*, Que Corporation, Carmel, 1990, p. 14.
9. Glossbrenner, A. and Anis, N., *Glossbrenner's Complete Hard Disk Handbook*, Osborne McGraw-Hill, Berkeley, 1990, p. 164.
10. Eischen, B., "US Legislation protects semi-conductor chips from piracy", *Canadian Computer Law Reporter*, Vol. 2 No. 3, 1985, p. 45.
11. Kratz, M.P.J., "Canada's integrated circuit topography act", *Canadian Computer Law Reporter*, Vol. 7 No. 3, 1990, p. 33.
12. Hoffman, L.J., *Rogue Programs, Viruses, Worms and Trojan Horses*, Van Nostrand Reinhold, New York, NY, 1990, p. 5.

Appendix: Glossary of terms

Bulletin board system
A computer system that is configured to receive communications via phone lines from computer users. These systems allow for exchange of information, electronic mail services and copying of computer files.

Computer hacking
The act and the method used to obtain valid user accounts on computer systems and the activity that occurs on the computer system once access has been obtained[6].

Default passwords
New systems when first installed often come with default or preset passwords that allow the computer system to be initially configured. Often, these passwords are not deleted from the system, thus leaving the system open to abuse by hackers.

Encryption
The translation of one character string into another by means of a cypher, translation table, or algorithm in order to render the information contained therein meaningless to anyone who does not possess the decoding mechanism[7].

Hard disk
High capacity computer disks that store data on rigid platters[8].

Local area network (LAN)
A computer and communications network that covers a limited geographical area, allows every node to communicate with every other node, and does not require a central node or processor[7, p. 346].

Low level format
The imposition of a magnetic structure on a computer disk. The read/write heads of a computer are used to divide the disk into tracks and sectors by recording bits that signify the sector address, and synchronize timing[9].

Node
Any station, terminal, computer or other device in a computer network[7, p. 348].

Password-cracking programs
Computer programs designed to defeat computer password security features. These programs work by trying various common passwords or by trying various combinations of letters and numbers.

Semi-conductor
The final or intermediate form of any product having two or more layers of metallic, insulating, or semi-conductor material deposited or otherwise placed on, or etched away or otherwise removed from, a piece of semi-conductor material in accordance with a predetermined pattern and intended to perform electronic circuitry function[10].

Topography
A three-dimensional matrix of electronic connections embodied in an electronic chip[11].

Virus
A computer program that is present on a computer system without the consent of the system owner. A virus has the capability of moving from one computer to another, of destroying and altering files and of denying computer service to legitimate users[12].

Write rings
Physical plastic or metallic rings that are affixed to computer tapes to prevent accidental overwriting of data contained therein.

Craig S. Hannaford is in charge of the Royal Canadian Mounted Police Technological Crime Section in Ottawa, Canada. He is a Certified General Accountant and has extensive experience in the investigation of computer-related crimes.