WHAT EVERYONE NEEDS TO KNOW ABOUT COMPUTER SECURITY

by

Lisa Ripley

August, 1984

INTRODUCTION

Computers are becoming increasingly important to accounting. General ledgers, cost accounting, and fixed assets can all be computerized. Microcomputers and electronic spreadsheets assist in the preparation of schedules for all facets of accounting.

As computer systems grow, the vulnerability of the system also grows. On a larger system, control over the system is more difficult to maintain. Unauthorized users may obtain valuable and confidential information. The vulnerability of the system is also apparent if the computer system breaks down. The activity of an entire department may be halted if the system is out of operation.

Keeping a computer system secure from break-in and break-down should be very important to a corporation that heavily depends on computers. Those people responsible for the operation of a computer system should be aware of computer security and controls.

In the December, 1982, issue of Dun's Business Month, the following passage dealing with computer security was found.

> Some years ago, several 13-year-olds at an East Coast school devised a way to cheat the Pepsi-Cola company. Their scheme was to tap into Pepsi's computer and direct it to send them free cases of Pepsi.
>
> Their school had a computer, and they were permitted to use it. Pleading ignorance and a great desire to learn, they simply asked their fathers how they used their office computers. The good old Dads--anxious to help--provided phone numbers, valid passwords and other critical information. By the time the kids were apprehended, they'd managed to crack a Canadian time-sharing facility with 22 commercial users and were well on the road to their modest goal of free Pepsi.[1]

Although the attempt was unsuccessful and the damage was limited, this serves as an example of how easy it could be to break into a computer system. This example is one of "about a hundred cases of computer fraud reported each year."[2]

COMPUTER CONTROLS

Having a secure computer system begins with computer controls. Controls can be divided into three areas: access controls, use controls, and threat monitoring. An issue of Data Management explains the three types of controls like this:

- Access Control — Don't let an interloper at your computing resources.
- Use Control — If he or she gets at them, don't let him or her use them.
- Threat Monitoring — If he or she gets at them and uses them, you had better know about it.[3]

The explanations may seem very basic, but they are steps that can be easily overlooked. Each of these controls is discussed in detail with examples of the control.

Access Controls

James Wade, a director of loss control and security says, "If we could enforce one single security principle, we could solve at once virtually all computer security problems. And that key is simply access control."[4]

Access controls can be of four different types: "restrictions on who can use the system, how they may use it, what they may use in the system, and where they may use it."[5] If the computer system is housed entirely in one room, a lock on the door to the room may restrict who can use the system.

Passwords can also be used to restrict who can use the system. If a password must be entered into the terminal before a user can gain access to a file, and the user does not know the current password, then access is restricted. Passwords should be changed periodically so their effectiveness at restricting access is maintained. The passwords should be short

enough so they can be remembered without writing them down, yet complex enough so that an unauthorized user could not easily guess the password.

Restrictions on how they may use the system and where they may use it can be created with key locks on the terminals. This is not a lock that requires a key, but instead is a terminal that can gain access to only certain files. An example of this would be the terminal in the payroll department could not gain access to the accounts payable system.

Restricted menus provide restrictions on what can be used on a system. Depending on the password given to the computer, the user will be allowed access only to certain files and programs. In the payroll department, the passwords used by the payroll clerks may present menus allowing access only to the program for entering the hours worked, while the password used by the payroll officer may allow him access to a program that could be used to change wage rates.

All of the access controls mentioned can be effective in keeping intruders off of the computer system. What happens if the intruder finds a way around the access controls? Use controls now become important.

Use Controls

The most common use control is encryption. Encryption involves storing data in "other than natural data format."[6] Data is stored on tape or disk using a special code and an encryption machine. Before the data may be used by the computer, the special code must be deciphered by the encryption machine, then the computer can read the data.

An effective use of encryption arises during transmission of data via communication lines. By having an encryption machine at the sending and receiving locations, encrypted data is transmitted. Anyone attempting to wiretap the communication line will not be able to read the data.

Use controls can be effective in keeping an intruder from using confidential data of the firm.

Threat Monitoring

Threat monitoring involves making sure the system operator knows who is using the system and whether or not the person is an authorized user. Threat monitoring controls the system after someone has gained access and used the system.

One firm created software to monitor actions of the computer system. The software controls the log-in procedure of the computer system and monitors any potential threats to the system.

> The software permits two abortive log-in attempts. But if the third attempt results in a failure, the software "informs" the prospective user that
>
> 1. his attempts to enter the system have failed,
> 2. the system operator is now monitoring his actions, and
> 3. the system will ignore any further log-in attempts, except for possible initiation of a call to the phone company for the purpose of tracing the source of the call if the person does not immediately hang up.[7]

Software such as this could be very effective in controlling a computer system.

All levels of control--access, use, and threat monitoring--are necessary for a computer system to be secure. If one level of control is broken through, another level should be present to prevent further intrusion.

COMPUTER LEGISLATION

If an intruder successfully breaks through all levels of control and commits a computer crime of some type, what can a corporation do to prosecute?

Computer crime legislation is beginning to be passed by states and the federal government. As of October, 1982, sixteen states had computer crime laws, and the Nelson Bill was in subcommittee hearings in the House of Representatives.[8]

Although the laws exist, the number of computer crimes that are prosecuted seems to be very low. Part of the problem may be proof. It is very hard to prove that data is stolen if a disk or tape is taken, copied, and then returned to its proper position. A case like this illustrates the importance of prevention. By preventing the crime, money and time can be saved.

CONCLUSION

The keys to prevention include the three types of controls already discussed, and a fourth type of control should be added--internal control. An article in the Harvard Business Review states the following:

> No one group should bear complete responsibility for protecting the computer system. The need for controls should be instilled in the entire organization, starting with top management and extending to all personnel.[9]

The accountants cannot be held responsible for the computer system security and neither can the data processing employees. As the article says, everyone is responsible. The corporation needs to work together and the belief that internal controls will lead to better security needs to be instilled in all employees.

Controls are the key to computer security, and with adequate controls, a computer system can be maintained securely.

ENDNOTES

[1] "Computer Security," Dun's Business Month, Dec. 1982, p. 94.

[2] Martin D.J. Buss and Lynn M. Salerno, "Common Sense and Computer Security," Harvard Business Review, March-April 1984, p. 112.

[3] Norman Statland, "Listen to Auditors Who Offer Low-Cost Data Security Procedures," Data Management, May 1982, p. 18.

[4] Dun's Business Month, p. 96.

[5] Avi Rushinek and Sara Rushinek, "Security: Vital Controls in an Accounting Information System," Accountancy, March 1983, p. 66.

[6] Statland, p. 20.

[7] Alan Hoffberg, "Protecting Your Computer System Against Unwanted Intrusion Need Not Be Expensive or Difficult," Office Administration and Automation, March 1984, p. 96.

[8] "Making Sense Out of Computer Crime Legislation," Data Management, Oct. 1982, p. 18.

[9] Buss, p. 121.

BIBLIOGRAPHY

Beitman, Lawrence. "A Practical Guide to Small Business Computer Security." The Office, August 1982, pp. 86-90.

Buss, Martin D.J., and Lynn M. Salerno. "Common Sense and Computer Security." Harvard Business Review, March-April 1984, pp. 112-121.

"Computer Security." Dun's Business Month, Dec. 1982, pp. 94-96.

Hoffberg, Alan. "Protecting Your Computer System Against Unwanted Intrusion Need Not Be Expensive or Difficult." Office Administration and Automation, March 1984, pp. 96-97.

"Making Sense Out of Computer Crime Legislation." Data Management, Oct. 1982, pp. 18-19+.

Mastromano, Frank, ed. "Management Information Systems." Management Accounting, August 1982, pp. 10, 66.

Mitchell, Derek. "The Software Solution to Prying Eyes." Accountancy, Dec. 1983, pp. 64-66.

Rushinek, Avi, and Sara Rushinek. "Security: Vital Controls in an Accounting Information System." Accountancy, March 1983, pp. 65-67.

Statland, Norman. "Listen to Auditors Who Offer Low-Cost Data Security Procedures." Data Management, May 1982, pp. 18-27.

Zimmerman, Philip, and George Daus. "Computer Security." The CPA Journal, Feb. 1984, pp. 75-76.