Journal of International Information Management

Volume 1 | Issue 1 Article 6

1992

The blossoming of data communications and the thorns of computer crimes: An analysis of the use and abuse of network computing

Michael T. Tang
Radford University

The blossoming of data communications and the thorns of computer crimes: An analysis of the use and abuse of network computing

Michael T. Tang
Radford University

ABSTRACT

The recent shift from mainframes to networking technologies has given business the ability to meet challenges in the competitive global markets with accurate, timely, and efficient data management. The blossoming of data communications, meanwhile, has created the potential thorns of computer crimes. This paper discusses the use and the impact of technology on the business environment, identifies various types of computer misconduct, and presents adequate systems measures for prevention. The paper concludes by enumerating various issues involved in effectively collaring the computer criminal.

INTRODUCTION

As information technologies advance, organizations and individuals depend more and more on the data available to make decisions and conduct business. Computers have become an important asset to a business firm because they can provide accurate and timely information for decision-making. Information has become an important means to success in the business community. Those who can make use of the company's most important data through computers have a better chance to survive in a highly competitive world.

Network technologies have progresssed through increasing levels of sophistication and resource distribution. The use of data communications to interconnect computerized storage devices and provide wide access to the databases has increased substantially. However, over the years, increasing use of computers to store, organize and retrieve data on demand has raised new concerns. The easiness of access and of manipulation of data through networks make the situation even worse. A recent study on 3,500 computer security professionals by the National Center for Computer Crime has found that computer crimes have cost U. S. companies more than $500 million a year (Bloombecker, 1989). Computer crimes have placed an extra heavy cost upon U. S. companies, who then transfer this cost to the consumers.

ILLUSTRATION UTILIZING NETWORK COMPUTING

Celco

The Hoechst-Celanese Corporation, the fibers plant in Narrows, Virginia, sometimes referred to as Celco, is an example of how computerized network systems have been applied to monitor the production and personnel operations. The distribution/receiving of information from all divisions wthin and without the plant is required to handle all data and information in a neat and orderly manner.

Since the merger of Hoechst and Celanese in 1986, the company has been booming economically and has moved up into the Fortune 100. The trend of handsome profits has continued since 1987. Dieter Zur Loye, CEO of the corporation, attributed the success to decreased competition from imports and the lower value of the dollar, stronger government enforcement of bilateral agreements, and record fiber consumption (Hoechst-Celanese Public Information Pamphlet).

After the merger in 1986, some new products were soon developed. The diversification helped the company become a sounder economic unit for investors and the corporation. The most interesting feature was an expansion into the software industry. Corporate Class Software was formed as a subsidiary to develop and market applications software to corporate end users. For example, Financial Application Solution to Analysis and Reporting (FASTAR) was initially developed for financial professionals to perform daily operations. It was originally developed as a mainframe-based solution to data gathering for financial reports. But, with the integration of more personal computers for managers, the specifications were changed to meet the business trends. It is designed to run on PCs allowing for collection, organization, management, and consolidation of financial data and to create summary reports (Datamation, 1989). Data can be loaded into FASTAR either manually or from micro-based software packages like Lotus 1-2-3 and dBASE, or from outside commercial database such as Dow Jones Retrieval.

In 1989, the corporation also diversified into the engineering plastics business for commercial usage. This included the use of certain forms of fiber optics to be used in automobiles of the future. The optical fiber network operates on quick bursts of light and electronics to control individual components such as locks, lights, engine systems, and power features from windows to seats (Design News, 1988). It could reduce the weight of the car and make the automobile more fuel efficient. This will probably revolutionize the automobile industry in the future since the addition of on-board computers is becoming standard. Wires will not be needed to connect accessories to options like anti-skid brakes, fuel injection systems, satellite navigation, collision avoidance devices and cellular telephones to name a few.

The processing of information to better serve customers is the backbone to Celco. Having multiple buildings on the plant site in Narrows creates a need to communicate effectively on site as well as with regional and head offices.

Celco is no exception to the trend to depart from mainframe to networks. When a mainframe, HP 3000, first started to work at Celco, it was the main style of computer systems throughout all industries. However, major changes within the information technology have

taken place at the plant. These included process control by PLCs/computer links; data is accessed by multiple numbers of end uses through networks and scheduling systems are now being done on the PCs. The PC has given managers the freedom to obtain information at a quicker pace and more accurately to serve their individual purposes. PCs are connected together on a network and specialized file servers do particular assignments such as managing database, electronic mail systems, or printers. The addition of voice mail systems on the internal phone network also has eliminated the problem of telephone tag. By attaching new workstations and file servers, communications between the Celco plant and other district offices can easily expand and adapt to the changing needs of business. This is done through the M.I.P.S. system, which handles purchase orders and production schedules at the present time.

An Ethernet-based local area network is being installed. This system will be using 10 Base T style with the building connecting the file server, an OS/2 based operating system, to the clients, which are MS/DOS based. This links together different departments working with CADs. As in all modern and effective businesses, information systems are playing an increasingly important role in the formulation of competitive strategies. With the integrated computer networking being formed and the present use of real time data, Celco is making a commitment to excellence through innovations in information systems.

Federal Express Packages Delivery Services

Federal Express has been a leader of innovation in the package delivery areas, setting standards for the entire industry in how a company can use information systems to train employees, trace packages from pickup to delivery, and conduct airplane maintenance.

The whole process of tracking a package starts with a hand-held terminal. The driver insures that the appropriate labels and codes are placed on for proper delivery. Then a bar code is put on the package with a light pen connected to a hand-held terminal. Vital statistics then are transmitted over radio waves from the terminal to a customer designed mainframe at the local dispatch office, then, via network, to headquarters in Memphis, Tennessee with the central databases residing on IBM mainframes (COSMOS). It then will be able to reveal the time for pickup, identification number, sender, destination, and arrival time. A package can be traced on-line from any station across the country. The interactive video system links more than 700 workstations to two central databases.

Federal Express has a unique way of transmitting important information to its employees by broadcasting every morning five minutes of corporate news and information. It then goes into basic statistics of the previous night's package volume, the company's closing stock prices, and an overview of the weather forecast, followed by operational information such as changes in company policies, billing systems, packaging procedures, etc. By developing so much of its resources toward information technology, Federal Express is preparing well for the future.

With innovations in information technology, business executives have been trying to figure out where they fit in and how a company should utilize information systems. Today we see the trend for corporations to link together all divisions through the use of networking. With some corporations not parting with their mainframes, the network would allow all divisions and each individual within the division, to access the mainframe and communicate with each other. They also allow the information systems division to control data and allow each divison to obtain information from each other with little or no manipulation.

Hospital Information Management

Medical facilities have been dominated mostly by the paper shuffling systems. The majority of the records have been on paper, including work orders, purchasing orders, billing forms and patient medical histories. Patients find themselves waiting while the staff searches for paperwork. This is quite time consuming and sometimes leads to being charged for tests never performed, unnecesssary services, and even being charged for another patient's account (Flanagan, 1988). Nurses are caught up with filling out documents and moving them along to the next stages, drawing them away from their medical duties.

PCs are increasingly becoming an intricate part of hospital information systems. PC's user friendliness, graphics capabilities and increased computing power are being recognized as backbones of useful LANs. With the installation of LANs, physicians can check on required information from their desktop PCs. This makes for better working conditions and less frustration among all segments of the work force. With the addition of optical disk storage medium linked to central databases, information can be retrieved in a much faster fashion.

Computers in most hospitals were used for financial aspects such as budgeting. Data processing was centralized. Marketing or financial planning were virtually non-existent for since there was not enough information for analysis. More hospitals today are moving away from just financial aspects to measuring productivity, costs, inventories and data storage. Staff members have direct access to relevant information and records. For example, well-planned pharmacy records must be maintained to control carefully the ordering, stocking, and distribution of drugs, and to avoid medication errors. Physicians can download information on a patient from a mainframe to track historical records, lab tests and other information from various departments.

The old way of information systems that hospitals operated was long, tedious and created unnecessary delays and inefficiency in performance. There is a close relationship between hospital survival and information systems because of the speed and reliability of information currently offered. With the integration of network computing information systems, hospitals are finding better ways to serve the patients. With the applications of Decision Support Systems and Expert Systems, information technology is offering a whole new era to hospitals and the health care industry.

TYPES OF NETWORK COMPUTER CRIMES

While there are many advantages of utilizing network computing, the greatest liability is the increase in computer crimes. Network computer crimes can be divided roughly into four large categories: financial fraud and theft, program theft, services theft, and vandalism (Gilbert, 1988).

Financial Fraud

Financial fraud and theft is the greatest and most widely recognized computer crime. It includes altering computer records to obtain money, stealing proprietary information stored in computers, and manipulating financial data to produce fraudulent financial reports. Items stolen or embezzled include assets, equipment, products, services, and many other company resources (Bequai, 1989). Pilferage schemes often take one or more of the following forms:

- Inventory lists doctored
- Cash sales tickets altered
- Merchandise shipped to the home of the deceitful employee
- Valuable materials substituted with cheaper ones
- Incorrect shipping labels
- Sales commissions and discounts altered
- Fictitious suppliers and customers created

Program Theft

A great deal of program theft is a result of what is known as the "differential association" theory. Most people feel that it is not necessarily a crime to copy computer programs from the office. They experience no guilt from engaging in this type of crime. By doing so, the owners of these programs suffer a loss. To compensate this loss, the prices of these programs are increased and then the legal users have to shoulder the burden of the cost for illegal ones.

Services Theft

The most common way of services theft is using the company's computer facility and time to do personal work. Gaining access to the confidential files of others without prior authorization is also considered data abuse. This form of crime sometimes entails a dishonest employee copying files and selling them to their company's competitors. Service theft can also take the form of a dishonest company employee inserting fraudulent data into the firm's computer for the purpose of creating fictitious claims such as life, health, accident, and casualty insurance cases.

Vandalism

Computer viruses have shown the ability to disrupt computer activities as thoroughly as a fire, flood, or tornado. Despite the fact that viruses may not be designed to do harm to the business community, they cause as much as $100 million dollars' worth of damages (Schwartz, 1990). The corruption of data by a virus could result in loss of computer time, waste of manpower, canceled orders, and loss of customer confidence.

Attacks on individual disk files are evolving into attempts to forbid the steady operations of entire communications networks. Most virus protection strategies are developed on the systems level. Access modifications are used to prevent data and programs from being modified. Even though there has been more hype than horror in the wake of recent tales about the villain programs (Karon, 1989), great emphasis has been placed on the protection of software. The following measures are often used to ensure safe software: employee development, independent programmer, software house, and hunter program.

WIRETAPPING OR EAVESDROPPING

As network computing becomes more popular, it brings a new meaning to the terms of wiretapping and eavesdropping. Companies that use networks of personal computers may be especially vulnerable. Data entry via terminals and networks can be used to gain inside information.

While networks give workers easier access to data and other computer resources, they can leave sensitive areas open to unauthorized penetration from inside and outside of the company. For example, every day networks are used to transmit close to one trillion U.S. dollars among financial institutions, and the value of critical information transmitted among corporations are often worth more than that. There are basically three types of data communications methodologies: the use of telephone wire, the packet network, and the local area network.

Telephone Wire

The use of telephone systems can be divided into two types: leased-line or dial-up. A leased-lne system is relatively secure because it links only authorized locations with each other which are maintained and monitored by telecommunication carriers. There is little chance that an outsider can break into the network. A dial-up system is relatively insecure. Since the phone number of these systems are published regularly by hacker magazines, outsiders can manage to bypass the password and get into the networks.

Packet Network

Packet networks are extensively used by most corporations. Information is sent through the same physical lines. The messages are assembled into packet assembler/dissembler process. Telenet, Tymnet, General Electric Information Services (GEIS), and Uninet are four of the most popular Packet networks in the U.S. Although some access securities are available, they are somewhat inadequate. Moreover, because it is connected to the public network through gateways, it becomes less secure.

Local Area Network

Local area networks are the special applications of data communication techniques within a limited geographical area. It connects authorized users throughout a local area by a special medium of cable. It is difficult to ensure that unauthorized users throughout a local area by a special medium of cable. It is difficult to ensure that unauthorized users are not receiving the message. As networks have grown in size and complexity (e.g., interface configuration, heterogeneous components), the major duties of local area network personnel often include control of operation and resources, planning for growth or service adjustment, and observation of its status and performance.

ESTABLISHING SYSTEMS CONTROLS

News media have cited many examples of hacker inroads into corporate and government databases through networks. Security provisions minimize many of these potential exposures, but the high visibility of such events demands greater care in assuring systems controls are in place. The obvious solution to the poor system controls is to restrict access to the computer networks. This, unfortunately, makes the computer operations more cumbersome; it also directly affects the cost of applications.

The majority of perpetrators who commit computer crimes are from within the organization. Furthermore, the level of computer expertise required to commit a fraud vary, but most require nothing more than a knowledge of how to use the existing system. Most fraud involves relatively simple schemes that take advantage of weaknesses in the existing systems control (Ernst & Whinney, 1987).

There are several measures that can be taken to improve systems control. First, the primary emphasis should be placed on the physical security aspect to prevent authorized access to the computer room, network command center, or communications equipment. Actual locks, keys or magnetically encoded cards can be used to activate terminals or doors. Detailed records of all accesses to the network should be kept by computers so that unauthorized access or altered information can be traced easily. Users should be required to log on to the network whenever they use a terminal by entering their unique identification codes. This record including names, I.D. number, date, time and terminal identification should be automatically recorded by the software in a central control file so that a complete record is kept of all users of the system. This information can also serve as daily operational control to ensure that daily activities are carried out properly.

Even if network access is secured with a call-back system and the database is protected with passwords, the computer system is still vulnerable when data is transmitted across telecommunication lines. For example, by tapping into the lines, unauthorized users can intrude a transmission and download the data to their own facilities. Encryption is usually used to protect data integrity during transmission through networks. Cryptography transforms information into nonreadable forms of data by randomly substituting streams of bits. This encrypted file can only be transformed back to the original form by using a special key. The key sets into motion a mathematical process that at the end "decrypts" the data.

An ID card with a magnetically encoded identifier can be used to claim for identification. After the claim is made, authentication can be done by using scanner examining extremely precise measurement of physical attributes such as fingerprint or eye-retina. Physical attributes used to identify users include fingerprints, signatures, voice/speech patterns, and palm geometry. Technologies for detecting physical attibutes are just beginning to materialize. Scanners that distinguish fingerprints or signatures are currently in use. Voice-input technologies have also made computer recognition of voice/speech patterns a popular technique.

A similar approach uses a token method. A token is a small device that contains a nonreadable key number. A user has to type in the user ID and activates the token with a personal identification number (PIN). Afterwards, the security control systems will send a random number to the user. Then the token is used to encrypt this random number by its internal number and sends the answer to the screen. Since the key of the token is nonreadable and buried within, it proves a very rigorous and effective method even though it is somewhat expensive.

The access of information can also be segregated by functions so that one can access only the authorized areas predefined by management. Furthermore, user location validation can be used to restrict access to some specific terminals to ensure segregation of duties. In addition, access time validation can also help to restrict specific access within certain time frames.

Security systems of the future will probably implement a combination of assured location and physical attributes identification. For instance, high-quality telephone lines might allow voice recognition as a cross-inspection while location might be verified by automatic call-back.

Software, as well as hardware, must be checked periodically to ensure that everything is working the way it was designed to function. Avoid locating a computer facility in an area frequented by outsiders. Even though the risk of infection cannot be eliminated, the following risk-reduction actions seem to be judicious:

- Restrict downloading of files and software from electronic bulletin boards.
- Limit the use of software products, including commercially developed packages. Avoid freeware or shareware not being independently verified to be virus free.
- Design interface to network gateways and other telecommunications ports that prevent direct access from outside-to-disk content.
- Segment data center-resident access storage device interconnection, reducing the possibility of virus infection of the central database.

Communication and environmental factors are also important in deterring network computer crimes. Computer criminals are tempted by money, influenced by relationships with colleagues, and swayed by stress at work (Reese, 1989). A periodical review of the working environment with a continued emphasis on the penalties for misuse of computer systems could help to deter computer crimes. Organizations need to take a tough stance on prosecuting dishonest employees, enforcing its rules and ethics codes vigorously.

SUGGESTED SANCTIONS

There are several effective sanctions proposed to combat computer crimes (Rosenblatt, 1990):

1. Confiscating the computing equipment of an offender;
2. Limiting/barring the use of computer systems by offenders;
3. Restricting the offender from sensitive positions in computing;
4. Implementing an active security awareness code of ethics, constantly reminding employees about their security responsibilities and the company's concern for security; and
5. Providing a clear set of performance measures for both management and staff.

TRADE-OFFS OF ECONOMICS VS. SECURITY

While the explosion of technology has increased management awareness of potential security infringement, economic components often limit the full implementation of safeguards. Many plans to ensure the physical and administration protection of data files and programs have been dropped because they were not cost-effective. Meanwhile the computer industry has been unwilling to assemble securities capabilities into their hardware and software, since the market was not ready to bear the cost of such sophisticated devices.

Management should determine how much protection investment can be afforded by considering the cost of precaution measures against the value of information itself. An awareness of security costs and their relationship to the significance of information will illuminate the economic dimension of security control.

CONCLUSIONS

The amount of investment needed to prevent computer crimes has increased. Computers and network technologies have contributed enormously to making data more accessible, increasing the potential for abuse. Future computer frauds are likely to continue to take advantage of the technological advances and the decentralization of electronic data processing. Corporations and financial institutions will continue to rely heavily on networks to transfer funds and vital information. As a result, computer fraud will spread into almost every organization through networks.

Computer crimes prevention will become more important in the future of information systems management. Companies should review their existing security systems control of their network to make sure that adequate measures are established for prevention. At the same time, government and industry should endorse specially-tailored proposals to deter computer criminals. This should include stiff criminal punishment for those caught producing or distributing computer viruses or participating in other computer crimes.

REFERENCES

Bequai, A. (1989). *How to Prevent Computer Crimes: A Guide for Managers.* New York: John Wiley and Sons, p. 33

Bloombecker, J. J. (1989, Oct. 1). Short-Circuiting Computer Crime. *Datamation,* pp. 71-73.

Datamation. (1989, February 15). p. 95.

Design News, (1988, December 15). p. 38.

Ernst & Whinney. (1987, June). Computer Fraud. *CPA Journal,* pp. 4-10.

Flanagan, H. (1988, June 5). Labs Integrate Hospital Information Systems. *Hospitals, 62,* 43.

Gilbert, J. (1988, November). Computer Crime: Detection and Prevention. *Journal of Property Management,* pp. 64-66.

Hoechst-Celanese Public Information Pamphlet.

Karon, P. (1989, May 31). The Hype Behind Computer Viruses: Their Bark May be Worse Than Their Byte. *PC Week,* p. 49.

Reese, F. F. (1989, September). Of Mice and Man. *Security Management,* pp. 89-91.

Rosenblatt, K. (1990, Feb.-March). Deterring Computer Crime. *Technology Review,* pp. 34-40.

Schwartz, M. (1990, Jan.-Feb.). Computer Security: Planning to Protect Corporate Assets. *Journal of Business Strategy,* pp. 38-42.