Review of Business, Vol. 16, No. 2, Winter 1994, pp. 24– 28

Protecting Information: Effective Security Controls

MARIE A. WRIGHT

Never before have there been greater security threats to the information stored in business and government computer systems. Information which was once vulnerable to unauthorized disclosure, modification, or destruction by a relatively small group of users within an organization now faces these same risks from the millions of individuals worldwide who use computer networks.

Information security requires more than the physical protection of computers. An effective information security program incorporates a combination of technological and human controls in order to *avoid* the loss of information, *deter* accidental or intentional unauthorized activities, *prevent* unauthorized data access, *detect* a loss or impending loss, *recover* after a loss has occurred, and *correct* system vulnerabilities to prevent the same loss from happening again (Parker, 1984).

Making computer and communication systems more secure is both a technological challenge and a managerial problem. The technology exists to incorporate adequate security safeguards within these systems, but the managerial demand for secure systems is virtually nonexistent outside of the defense and financial industries. That so many of our commercial systems provide marginal security at best is a reflection of the lack of managerial awareness and understanding of the need to protect the information stored in, and transmitted between, computers. The economic ramifications of inadequate security can be significant. Consider the following examples:

- Volkswagen lost almost $260 million as the result of an insider scam that created phony currency-exchange transactions and then covered them with real transactions a few days later, pocketing the float as the exchange rate was changing (Neumann, 1992).
- The Bank of New York experienced a $32 billion overdraft as the result of a processing error that went unchecked. The bank had to borrow $24 billion to cover its transactions for one day, and paid $5 million for the day's interest (Neumann, 1991).
- When the government of India requested bids on a billion-dollar contract for jet fighters, French intelligence agents stole bid information submitted by the United States and gave it to a French firm competing for the contract. The proprietary information helped the French company to win the contract (Mello, 1992).
- A group of hackers, operating under the name *Masters of Deception*, victimized such companies as Southwestern Bell, New York Telephone Company, Pacific Bell, US West, TRW Inc., Information America Inc., Martin Marietta Electronics Information and Missile Group, ITT Corporation, Educational Broadcast Corporation, Bugle Boy, New York University, and the University of Washington. The hackers stole credit reports, and altered or deleted files at some sites. Southwestern Bell alone reportedly spent $370,000 to repair corrupted programs and to buy more secure hardware and software (Kaplan & Clyde, 1993).

All organizations face the risk of a breach in information security. Although no system can be completely secure, most security breaches can be prevented, or their impact minimized, with the implementation of effective technologi-

Marie A. Wright is Associate Professor in the Management Information Systems Department, Ancell School of Business, at Western Connecticut State University, Danbury, CT.

cal and human controls. This article identifies five categories of security controls: administrative, personnel, physical, logical, and data communications. When used in combination, these controls provide an acceptable level of protection for sensitive information.

Administrative Security Control

Information security must originate from the top. If senior management does not mandate the establishment of operational and accountability procedures, constraints, and supplementary controls necessary to protect the company's information, the viability of the organization will be at stake.

Not all information must be secured. In fact, the cost to completely secure all information would be prohibitive. However, it is management's responsibility to identify the quantity, type, and sensitivity of the information to be protected, and to determine the point at which the cost to protect the information exceeds its value.

Administrative control requires a comprehensive security plan be established before a crisis occurs. Senior management should establish a steering committee, composed of representatives from the user community, information systems and security departments, and audit staff, to be responsible for developing, publicizing, reviewing, and evaluating the organization's security policies and procedures. Some administrative controls which should be included are as follows:

- Establish appropriate hiring procedures. References and background checks should be performed as a matter of routine.
- Assign individual accountability for the data. Functional responsibilities for network managers, technical staff, operations staff, and users should be established.
- Maintain an ongoing security awareness and education program. Employee performance should be evaluated on a periodic basis, with penalties for noncompliance, or rewards for superior performance.
- Provide grievance channels for all employees.
- Develop and practice a disaster recovery plan. Include provisions which ensure that all programs and data are routinely backed-up and stored offsite. Designate a computer emergency response team in conjunction with this plan.
- Establish audit provisions to ensure compliance with corporate security policies. Systems development procedures, software coding, testing and installation methodologies, and training materials should be reviewed, and user activities and authorization records should be compared.

Ironically, the most significant hindrance to administrative control may be management itself. According to a 1993 *Infosecurity News*' survey of information systems security professionals, the biggest obstacle to information security continues to be the lack of awareness about the need to protect information. All too often, security controls are dismissed as unnecessary expenses which inhibit employee productivity.

The importance of effective administrative control is likely to become greater in the future due to the increase in public awareness of computer abuse, the potential for larger losses as computer networks become further interconnected, and the increased risk of personal liability which could be imposed upon top management when inadequate security controls are found to exist.

Personnel Security Control

Employees pose the greatest challenge to information security because it is particularly difficult to prevent or detect employee crime when fraudulent activities are hidden by legitimate transactions. According to a 1991 report by the National Computer System Security and Privacy Advisory Board, insider crimes cost nearly ten times as much as those committed by outsiders. While most losses are attributed to human errors, accidents, or omissions, an increasing percentage is ascribed to the fraudulent actions of dishonest or disgruntled employees. In many cases, the losses are the result of missing or inadequate managerial controls, procedures, and supervision.

One of the most revealing studies on personnel security was conducted in 1986 by the Computer Security Task Force established by the Presidential Council on Integrity and Efficiency. Although the study focused on former government employees convicted of computer fraud, the findings provided insight into the human factors which underlie information security. A surprising profile was generated:

- The convicted criminals were considered good employees. They had been with their respective agencies for an average of five years before committing their crimes, and during that five-year period, most had been promoted.
- The most common crime committed was data diddling: illegally modifying input data in order to generate fraudulent negotiable financial instruments as output.
- Most of the former employees reported that they stole because of situational stresses: medical bills, indebtedness, imminent eviction, or loss of a spouse's income. Others were disgruntled, or stole because a known vulnerability existed in the system and they could not resist the temptation.
- The crimes were committed primarily because the employees believed that controls were inadequate.

> Managerial supervision was weak either because the supervisors were too busy to review their subordinates' work, or because the individuals involved were believed to be trusted employees. Some of these individuals reported that their supervisors had never learned the automated versions of the jobs which had previously been done manually, and so the employees were able to take advantage of their superiors' ignorance.

While employees may be the main problem when it comes to security, they also can be a significant part of the solution. Most employees will do what management intends, so it is critical that the commitment to security be consistently demonstrated and reinforced. The importance of ongoing employee security training cannot be overemphasized; all employees must be made aware of the potential threats to information security, as well as their responsibilities to protect the organization's information, before any security program can succeed.

Physical Security Control

Of all the problems which threaten computer operations, those affecting the physical environment are perhaps the easiest to comprehend. Physical security is concerned with protecting the facilities, equipment, and information from natural disasters and malicious destruction. These controls incorporate a number of visible defenses which provide an outer perimeter of security. Locks, guards, badges, and surveillance devices (such as closed circuit television) are often used to control access to buildings, computer centers, telecommunication facilities, storage areas, or control rooms. Access through door or gate entrance points can be restricted by equipping these entrances with front-end equipment, such as readers which are activated by employee cards or keys. Personnel and visitor traffic can be further regulated through the use of biometric devices, which use technology to recognize retina patterns, hand prints, fingerprints, or voice patterns.

Contingency planning is critical for an organization to respond to the myriad accidents or disasters which could occur: fire, flood, theft, explosion, power failure, electrical disturbances, employee sickness or death, terrorist attack, labor strikes, aircraft or vehicle impact, environmental hazards, earthquakes, volcanoes, avalanches, hacker activities, or computer viruses. Recovery from such phenomena requires the establishment of backup procedures, personnel responsibilities, alternative processing and communication facilities, testing plans, and insurance coverage before a catastrophe occurs. Although a detailed disaster recovery plan should be part of an organization's overall security program, successful recovery requires the procedures be understood, reviewed, and practiced by all employees.

Logical Security Control

Logical security provides a finer layer of information protection by functioning within the perimeter of physical security. Logical security is provided by the operating system to protect the information stored in, or connected to, a computer. The operating system is the main line of defense against the unauthorized use of system files or programs because the protective mechanisms in most operating systems enforce rules concerning user access and processing rights. These constraints are imposed through the use of system and data access controls.

System access controls rely upon a process of identification and authentication to restrict system access and to monitor user activities. A conventional login identifier, such as a name or account number, is typically entered by a user for identification purposes. Once the login identifier is authenticated, it is used to record the user's activities in an audit trail. Authentication can be accomplished through the use of a key, token, smart card, or badge, although the most frequently used authentication technique requires the user to enter a secret password.

Data access controls use both discretionary and mandatory access controls to further protect information once system access has been achieved. Discretionary access control allows a user to identify those who can access the user's data, and to specify the allowable data access rights (e.g., read or write). Mandatory access control is enforced by the operating system at all times, and cannot be subjectively modified by a user. This type of control restricts information access according to the sensitivity of the information and the level of trust associated with the user.

Closely related to the concept of access control is the principle of least privilege, where each user should be granted the minimum access authorization necessary to perform a given task. The application of this principle limits the damage which can result from accidents, errors, or unauthorized use.

Access controls are not foolproof. In fact, the misuse of passwords has become so commonplace that management should adopt measures to ensure that passwords provide the necessary degree of security. Some time-honored principles of password management follow:

- A password should be easy to remember but hard to guess. A pronounceable nonsense word, (such as "yerdeloo"), at least eight characters in length, is often a good choice. Not recommended is a numeric password, such as the user's telephone number or social security number.
- Passwords should never be written down, shared, stored on-line, or transmitted via electronic mail.
- All passwords should be changed on a regular basis.

- A password should be deactivated whenever a user quits, retires, is transferred, or is terminated.

All employees must be made aware of the importance of password security, and should be informed of the repercussions if their passwords are not protected.

Data Communications Security Control

Microcomputers and networks have become the foundation of business life. According to the National Computer Security Association, more than half of the sixty million microcomputers used by U.S. businesses are connected to networks. Network resources allow worldwide access to information, no matter where it resides, or where the users are located. Unfortunately, the physical and logical controls used by an organization to secure its information offer no protection when that information is being electronically transmitted.

Threats to communication security are posed by individuals outside of an organization, and their attacks can be active or passive. Active attacks intentionally cause the transmitted information to be changed. For example, an intruder could make undetected and unauthorized modifications to the contents of a transmitted message. Information may be deleted or delayed, or changes could be made to the order in which a series of messages are transmitted. The destination address of a message could be changed, causing the message to be directed to another party. Or the origination address could be altered, causing the receiver of the message to believe that the transmission was sent from a different source. Legitimate messages could be recorded and later played back, allowing an unauthorized user to establish a connection under a false identity, or causing a transaction to be performed twice. Active attacks are easier to detect than to prevent.

Passive attacks result in the unauthorized disclosure of transmitted information. Passive threats to security arise whenever messages are intercepted and read by outsiders. In some cases, the mere existence of message traffic is important to an intruder because the pattern of messages may reveal the amount of business being transacted between different users. Passive attacks are easier to prevent than to detect.

The only way to protect transmitted information is through the use of encryption. The mathematical process of encryption uses a key to transform information to an unintelligible form in order to prevent its unauthorized disclosure or modification.

Several encryption alternatives are available. One of the oldest and most widely used cryptographic systems in the United States is the Data Encryption Standard (DES). The DES has been an industry staple for more than fifteen years, and it is used extensively by financial institutions for the encryption of financial transactions. A private key encryption algorithm, the DES uses the same key to encipher and decipher a message. The key must be kept secret, and changed frequently, so that the integrity of the transmitted message is not compromised.

Other encryption algorithms use two different keys to control the encryption and decryption operations. Public key encryption algorithms, such as the RSA algorithm, typically use a public key to encipher a message and a private key to decipher the message. The strength of the RSA algorithm resides in the computational infeasibility of calculating the private key from the public key. The RSA algorithm is recognized internationally as the public key encryption standard, and it is currently used by more than two-thirds of the U.S. computer industry.

> " . . . the biggest obstacle to information security continues to be the lack of awareness about the need to protect information."

The most recent development in cryptographic alternatives is the federal government's key escrow encryption initiative, more popularly known as the Clipper Chip and the Capstone chip. The Clipper Chip is a private key encryption algorithm contained on a chip. Its complement, the Capstone chip, uses a public key encryption algorithm. Inherent to both chipsets is a controversial key escrow system which requires that the decryption keys of all Clipper Chip and Capstone encryption products sold be registered with two government-approved agencies. The decryption keys could be retrieved through court order, enabling government officials to eavesdrop on encrypted communications for law enforcement or national security purposes.

The key escrow encryption initiative is enshrouded in controversy. Of paramount concern is the perceived threat to individual privacy and corporate security. Public confidence in the Capstone and Clipper Chips has been difficult to achieve because the underlying technology remains classified. The secrecy surrounding this technology has fostered doubts about the strength of the algorithm, and fears that the chips could be reverse-engineered in time.

Questions have been raised about the impact of this technology on business. Of immediate concern is the public's forced reliance upon a single, government-approved supplier of the chips. Mykotronx, Inc. currently maintains exclusive rights to manufacture and market the chipsets. Because the Clipper Chip and Capstone algorithms do not comply with existing international standards, there are concerns that the added investment in hardware and personnel could make the technology unduly expensive to implement. There are worries that foreign companies may not be able to get the chips, and that foreign reaction to the U.S. government holding the decryption keys may be unfavorable. These worries are compounded by other security fears: the keys could be compromised during manufacturing, while being transported to the government-approved agencies, or while stored in escrow.

Management should seek expert advice before selecting and implementing any system of encryption. In order to do this, management must be aware of the threats to communication security, and should incorporate encryption into the overall security plan.

Summary

Effective security measures are required to adequately protect an organization's information against the risks of disclosure, modification, or deletion. A comprehensive security program should include administrative, personnel, physical, logical, and data communications security controls, and should exemplify management's awareness and understanding of the need to protect information.

References

Kaplan, R. and Clyde, R. (1993). "Learning from Loss: Classic VMS Security Breaches," *InfoSecurity News*, (May/June), pp. 28-29.

Mello, J.P. (1992). "Espionage! Are the Spooks Targeting Your Business?" *InfoSecurity Product News*, (September/October), pp. 1-10.

Neumann, P.G. (1991). "Expecting the Unexpected," *Communications of the ACM*, (May), p. 128.

Neumann, P.G. (1992). "Fraud by Computer," *Communications of the ACM*, (August), p. 154.

Parker, D.B. (1984). "The Many Faces of Data Vulnerability," *IEEE Spectrum*, (May), pp. 46-49.