Facilities Management in the Age of Information Warfare[1]

by M. E. Kabay, Ph.D.

Associate Professor, Information Assurance
Program Director, Master of Science in Information Assurance
Norwich University, Northfield, VT 05663-1035 USA

Facilities managers have always been involved in security. Many sites provide their tenants with guard services, access control systems, and surveillance. However, as the developed world increases its reliance on information systems, facilities managers are being called upon to help their clients establish stronger security for information resources.

This article summarizes some of the changes that have been taking place in information systems security in the last few years and then turns to some practical steps facilities managers can take to provide better security to existing tenants and to make their site more attractive to prospective tenants. In the text that follows, I shall refer to "clients" but naturally also include organizations that have their own, in-house facilities managers. Service-oriented facilities manager always treat their tenants as clients even if they work for the same organization.

Information Security Is Changing its Perspectives

The defining technology of civilization as we enter the twenty-first century is the computer. Computers are pervasive, necessary and vulnerable to attack. Computers are linked to each other through networks; one cannot pick up a daily newspaper without reading about the data superhighway that will supposedly bring cyberspace into our living rooms and allegedly bring anything from good grades to the end of civilization.

In the closing years of our century, the developed world depends on information technology to a degree unimagined ever a few years ago. Cellular phones depend on computers to switch their signals from station to station. Automobiles can't run without microprocessors. Air traffic, ground transport, medical care, science, the military, consumer goods – all depend on information technology. Factories communicate automatically using EDI (electronic data interchange) so that suppliers can deliver materials and parts minutes before they are needed by the client. The use of computers and telecommunications links for communications has spawned a new sphere of human intercourse: cyberspace.

Cyberspace includes all the intangible communications that many of us depend on daily: from voice messaging systems through electronic bulletin boards, CompuServe and the Internet, digital telephony and virtual reality. Because of the storage and transmission of information about

1 This paper was originally published in *Facilities Management* magazine in 1996.

ourselves, we all extend at least partly into cyberspace. An error in a government computer can cause untold headaches for the victims of mistaken identity. An error in a commercial credit bureau can ruin an innocent person's chances of buying a car.

In contrast with earlier times, computer expertise is no longer rare. Some children begin using computers as early as three years of age. One computer expert in Los Angeles was writing programs at eight and had his first contract with a major computer manufacturer as a consultant at the age of thirteen. He was hired for his deep knowledge of the operating system for million-dollar computers. By the age of sixteen, he was a millionaire because of a utility program he wrote that was sold to thousands of customers at $5000 a copy.

Cyberspace has its villains, too. Disturbed, poorly socialized youths turn the world of electronic communications into the equivalent of the trash-strewn school yard. Childish criminal hackers – including children – enter poorly-protected systems and leave electronic graffiti in their wake. Misguided programmers amuse themselves by writing self-replicating programs called viruses which cause havoc on infected systems. Government agents invade privacy, interfere with citizens' rights to private communication and store intimate details of the lives of innocent and guilty alike.

Organized crime is implicated in a growing number of attacks on computer systems. In response, the FBI created a special unit, the Computer Analysis and Response Team (CART) in February 1994. CART consists of computer specialists devoted to the identification and preservation of computer data needed as evidence in criminal prosecutions.

Another area of concern is the growing use of the Internet and of value-added services such as CompuServe and America Online. Criminals have already taken advantage of the relative anonymity of cyberspace communications to engage in fraud.

The Mission of INFOSEC

The classic definition of information security is

> "Data security ... [involves] the protection of information from unauthorized or accidental modification, destruction and disclosure."

Another classic triad names confidentiality, integrity and availability. Donn B. Parker, a respected author, teacher and thinker in the security field, added to this triad another three factors: possession, authenticity and utility, making the *Parkerian Hexad*. The following list defines each of the terms used above:

- *Protection* means reducing the likelihood and severity of damage. Another way of putting this is that information security strives to reduce risks. It is not possible in practice to provide perfect prevention of security violations. Common sense suggests that the degree of protection must match the value of the data.

- *Information* is protected by caring for its form, content and storage medium.

- *Unauthorized* means forbidden or undocumented. The very concept of authorization implies classification: there must be some definition of which data are to be protected and at what level.

- *Accidents* account for a major proportion of data damage. Accidents are due mostly to ignorance or to carelessness. Management must either hire well trained, knowledgeable staff or provide appropriate on-the-job training. In either case, part of the task facing all managers is to create, maintain and enhance motivation to do a good job. These basic management issues profoundly affect enterprise security.

- *Modification* means changes of any kind. The ultimate modification is *destruction.* However, you can usually spot destruction fairly easily. With adequate backups copies, data can be restored quickly. A more serious problem is small but significant changes in data. The work required to find the changes is often a greater problem than the changes themselves. Computer viruses that wipe a hard disk identify themselves at once and can be removed quickly. Viruses that make small random changes can persist for months, ruin the integrity of backups, and end up costing the victim more than the virulent disk destroyers.

- *Disclosure* means allowing unauthorized people to see or use data. Again, this word implies the need for a system of data classification. Who can see which data and when?

- *Confidentiality* is a wider concept than disclosure. For example, certain files may be confidential; the data owner may impose operating system controls to restrict access to the data in the files. Nevertheless, it may be possible for an unauthorized person to see the names of these files or find out how often they are accessed. Changing a file's security status may be a breach of confidentiality. Copying data from a secure file to an unsecured file is a breach of confidentiality.

- *Possession* means control over information. When thieves copy proprietary software without authorization, they are breaching the owner's possession of the software.

- *Integrity* refers to internal consistency. A database is termed structurally corrupt when its internal pointers or indexes no longer correspond to the actual records they point to. For example, if the next record in a group is in position 123 but the index pointer refers to position 234, the structure lacks integrity. Surreptitiously using a disk editor to bypass security and alter pointers in such a data structure would impair integrity even if all the data records were left intact. Logical corruption occurs when data are inconsistent with each other or with system constraints. For example, if the summary field in an order header contains a total of $5,678 for all items purchased but the actual sum of the costs is $6,789 then the data structure is logically corrupt; it lacks integrity.

- *Authenticity* refers to correspondence between data and what the data represent. For example, if a field is supposed to contain the number of parking violations cited by a specific police officer, then the field should not contain an outdated record of parking violations or the number of arrests by that officer. Another example of impaired authenticity is electronic mail sent with a false name. The only breach of security in such a case is loss of authenticity.

- *Availability* means that data can be gotten to; they are accessible in a timely fashion, convenient, handy. If a server crashes, the data on its disks are no longer available; but if a mirror disk is at hand, the data may still be available.

- *Utility* refers to the usefulness of data for specific purposes. Even if the information is still intact, it may have been transformed into a less useful form. Parker gives as an example the unauthorized conversion of monetary values in a database; seeing employees' salaries in foreign currency reduces the utility of the data. One of my colleagues was called in to help a firm whose source code had all been encrypted by a departing programmer. The programmer claimed to have done so to protect his ex-employer's security, but unfortunately claimed to have forgotten the encryption key. In a formal sense, the data were authentic, accurate and available – they just were not useful.

Threats to Information

Enterprise systems are faced with two kinds of threat: people and disasters. People include managers, employees, service personnel, temporary workers, suppliers, clients, thieves, liars and frauds. Disasters include fire, flood, earthquake, civil disturbance and war.

Most of the damage to information system is caused by errors and omissions of staff who are authorized to use the systems they damage. Carelessness, inattention, inadequate training and inadequate supervision are responsible for more than half of all the damage to information technology.

Intentional attacks on information may have different motivations and targets. To make sense of the wide range of problems we face in resisting deliberate attacks on information systems, Winn Schwartau, a leading information warfare theorist, has defined three levels of information warfare:

- Level one: interpersonal damage. Damage to individuals in recent cases includes impersonation in cyberspace (e.g., false attribution of damaging communications), appropriation of credit records (for fraud and theft), harassment (e.g., interruption of phone services) and loss of privacy (e.g., theft of medical records).

- Level two: intercorporate damage. Attacks on the financial and operational interests of corporations, government departments, universities and so on. Such attacks include industrial espionage, theft of services or money, and sabotage.

- Level three: international and inter-trading block damage. Destabilization of entire economies and societies. The techniques of information warfare levels one and two could be applied in a systematic way by terrorists, extortionists, or foreign governments.

This introductory article cannot go into detailed descriptions of all the techniques used for information warfare; instead, we will look at those techniques which should most concern facilities managers: penetration of security perimeters.

Social Engineering

Breaching security perimeters is the first step in many, but not all, attacks on I.T. Attackers, especially criminal hackers, have developed a range of techniques generally called "social engineering." Many techniques involve eavesdropping, or unauthorized listening to communications. Weak access controls give many intruders a nearly open door into data processing and communications systems; brute-force attacks target harder perimeters. Traffic analysis, a component of SIGINT, or signals intelligence, allows an observer to deduce important information by monitoring communications flows. Finally, data leakage is the practically undetectable loss of control over or possession of information.

Social engineering often begins with scavenging, the search through discarded materials for nuggets of valuable information. Scavengers (also known as Dumpster divers when they root through real garbage) are especially interested in security information that can help them penetrate the perimeter using identification and authentication data. Logon IDs (identification) and their passwords (authentication, or proof of legitimate use of the ID) are prizes in this search.

Social engineering's most powerful and commonly-used technique is impersonation. Impersonation can occur on the human level or electronically. For example, *piggybacking* consists of entering a secure area at the same time as an authorized user. When an employee slips an ID card through the reader and politely ushers a colleague through the door first, the pair have fooled the security system into allowing two people into the area on one ID. Similarly, when users leave work stations logged into a network without putting up a security screen, they have encouraged logical piggybacking into the network. Both forms of piggybacking are made easier by psychosocial factors which impede the implementation of security policies. Most people are socialized into holding doors open for others, so letting one's colleague (or a visitor) in through a security screen may not even register in the perpetrator's mind as a violation of security: it's just normal politeness. Blanking one's screen and locking it before getting up for a coffee may make a naive user uncomfortable: it implies lack of trust of colleagues, and society teaches people to value trust. Appropriate awareness training and practice can overcome these inappropriate scruples.

Building staff can contribute to a more secure environment by enforcing requirements to wear employee-identification badges, scrupulously checking on inbound and outbound strangers, and by being alert to and reporting unusual activities spotted during patrols and CCTV surveillance.

Data Leakage

Perhaps the most pervasive and subtle attack of all is data leakage – the insensible copying of restricted information. The main reason information can be stolen so easily is poor data security among users and administrators of work stations (the term personal computer should have been banned from office environments because of the false impression it creates). Such systems have standardized data formats (e.g., spreadsheet, database and word-processing files) that can easily be read on millions of systems around the world. In contrast, mainframe files tend to be in proprietary or site-specific formats which are considerably more expensive to convert and use. In addition, work stations often have high-capacity miniature media such as 1.44 Mb (megabyte, or millions of characters) diskettes a few cm in diameter (recent products can put 10 Mb on a diskette) or removable disk drives holding up to a GB (gigabyte, or approximately 10^9 characters) on units that

can be concealed in a pocket. Typically, work stations have limited or no physical controls against data theft; they rarely have access-control software installed.

Some simple precautions can make data theft less likely. Clearly labeling all removable media with tags that indicate their level of sensitivity and their ownership would make *accidental* removal of such media less excusable. Certainly facilities managers can safeguard their own site records; use adequate access controls for the security computers and for administrative computers containing information about the buildings and clients. Security programs on each workstation can prevent unauthorized access to the computer and control use of the diskette drives; the auditing features of such programs can provide a record of all activity by each user ID and by so doing further discourage casual data theft. If the facility provides central guard stations, clients may agree to have the staff check magnetic and optical media for authorization before allowing removal.

Wiretaps

Another area of concern to facilities staff is protection of telephone and network cabling against unauthorized wiretaps. Junction panels must be secured at all times to prevent tampering; cables should run through manifolds to prevent attachment of taps outside authorized locations.

In addition, anyone concerned about security should ban wireless phones from their premises; these devices broadcast all communications to a radius of hundreds of yards for pickup by anyone with a compatible handset or broad-range scanner. Similarly, cellular phones are not secure and all calls made using these systems should be considered public.

Personnel Issues

Much of the above overview has been concerned with technical issues. However, at the heart of all security is trust in people. It is critically important that all staff hired by the facilities manager be thoroughly screened for suitable background. Cleaning staff, guards, maintenance personnel – all have access to secure areas maintained by clients; the facilities management group's reputation rests in the trustworthiness and honesty of all such staff.

In a recent case in Florida, two computers disappeared from a medical clinic; their disks contained the clinical records of 8,000 people who were HIV-positive. The disappearance of the computers was met with dismay by everyone concerned, given the possible damage to people's lives from unauthorized publication of their status. The computers were eventually located: they had been stolen by two security guards assigned to protect the clinic. Facilities managers should contemplate the embarrassment and legal liability of the firm that supplied those guards.