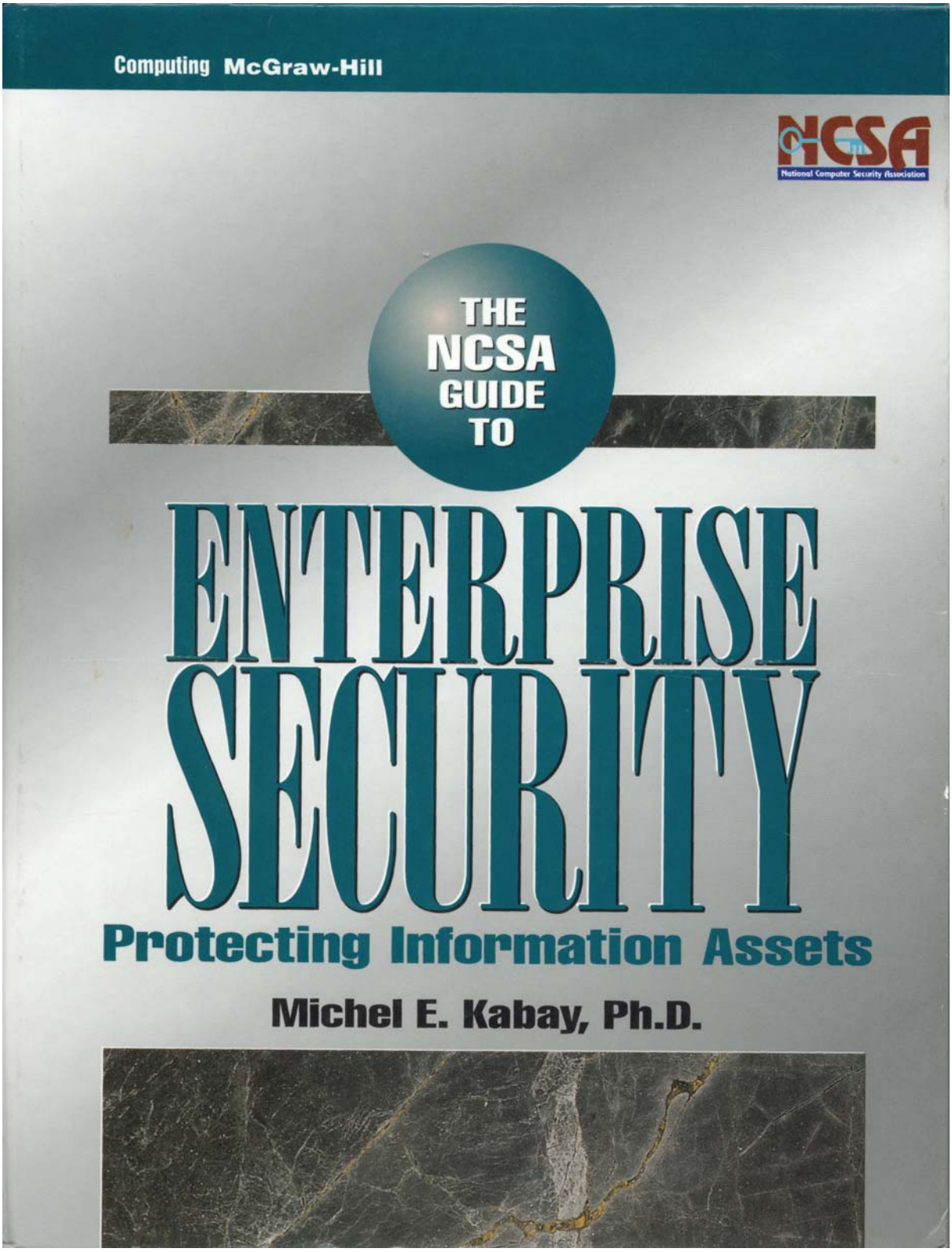

LAST MODIFIED: October 3, 1995

NCSA Guide to Enterprise Security

Table of Contents

Objectives: 3

What is enterprise systems security? 3

History 8

The mission 10

Definitions 11

Threats to security 12

The problem of ascertainment 12

Threats from insiders 13

Threats from outsiders 14

Statistics 15

Information warfare 15

Historical perspective 15

Conceptual framework 16

Risk assessment 17

Critical and sensitive data 17

Quantitative risk analysis 18

Qualitative risk analysis 20

Risk analysis in the age of information warfare 20

Summary 21

CHAPTER NOTES 22

Note: This is the original MS used for the textbook published in 1996. It differs from the published version in minor details.

Chapter 1: Introduction—protecting your information assets

Information is recognized as a strategic asset in today's competitive world. Threats to enterprise information systems must be met by appropriate responses. This text teaches the concepts, vocabulary and practice of information technology security for people immersed in the day-to-day tasks of managing information systems and also for students beginning their study of information security. The focus is on *enterprise* systems security, as distinct from the techniques required for specific platforms. There are many security texts available for learning the syntax required to define password length on a particular version of a local area network; this text explains why one should bother and how to convince managers and employees to care about the issue.

The **National Computer Security Association** serves as a clearing house for information about information systems security (infosec). This text is one of a series of *NCSA Guides* covering infosec topics. It serves participants in the NCSA *Information Technology Security* course and is suitable for practitioners involved in the management and application of information technology as well as college and university courses introducing information security to students at the undergraduate level and in business administration programs.

Objectives:

After studying this chapter, the reader should be able to
1. define the key concerns of enterprise systems security.
2. set information security in an historical context.
3. define the mission of the information security practitioner.
4. present industry statistics on the prevalence of computer and telecommunications crime.
5. describe methods for assessing vulnerability and risk.

What is enterprise systems security?

Enterprise systems are the computers and networks on which society increasingly depends for information management, process control, and direct control of equipment. The consequences of damage to or loss of information affects every sector of society. Not only commerce, education, and business are at risk; the political process itself may be attacked as computerized voting systems become more widespread.

We face an uphill battle whenever we try to convince management of the need for appropriate information systems security measures. Security is seen as a kind of insurance — it's necessary but boring. Insurance is thought of as an expense rather than as an investment. In contrast, this

text is based on the premise that enterprise systems security protects against disaster instead of simply paying for recovery.

There is a growing consensus: information security matters. In 1988, the Defense Advanced Research Projects Agency (DARPA) asked the Computer Science and Technology Board (renamed the Computer Science and Telecommunications Board of the NRC in 1990) for a study of computer and communications security issues affecting U.S. government and industry. The NRC's System Security Study Committee published its results in a readable and informative book, *Computers at Risk: Safe Computing in the Information Age.*

The Committee included experts with impeccable credentials, including executives from major computer vendors such as HP, DEC and IBM; from high-technology companies such as Shearson, Lehman, Hutton Inc. and Rockwell International; universities such as Harvard and MIT; and think tanks like the RAND Corporation.

A public misconception is the supposed divergence in focus of the military and of commerce: the military is usually described as concerned with external threats and the problem of disclosure, whereas businesses are said to worry more about insider threats to data integrity. On the contrary, the military and commerce need to protect data in similar ways. The differences arise primarily from (1) the sophistication and resources available to governments that try to crack foreign military systems; (2) the relatively strong military emphasis on prevention compared with commercial need for proof that can be used in legal proceedings; and (3) the availability to the military of deep background checks on personnel contrasted with the limits imposed on the invasion of privacy in the commercial sector.

Some of the more interesting general points raised by the NRC Committee include:

- because of the rapid and discontinuous pace of innovation in the computer field, ‘with respect to computer security, the past is not a good predictor of the future;’

- embedded systems (those where the microprocessor is not accessible to reprogramming by the user; e.g., medical imaging systems) open us to greater risks from inadequate quality assurance (e.g., a software bug in a Therac 25 linear accelerator killed three patients by irradiating them with more than 100 times the intended radiation dosage);

- networking makes it possible to harm many more systems: ‘Interconnection gives an almost ecological flavor to security; it creates dependencies that can harm as well as benefit the community....’

The Committee proposed six major recommendations, summarized as follows:

1) Push for implementation of generally accepted system security principles:

- quality assurance standards that include security considerations;

- access control for operations as well as data [e.g., any of the menu systems which preclude access to the operating system];

- unambiguous user identification (ID) and authentication [e.g., personal profiles and hand-held password generators]

- protection of executable code [e.g., flags to show that certain object modules are 'production' or 'installed' and thus apply strict access control that would prevent unauthorized modification — as found in configuration control systems]

- security logging [e.g., logging failed file-open attempts and logon password violations];

- assigning a security administrator to each enterprise;

- data encryption;

- operational support tools for verifying the state and effectiveness of security measures [e.g., audit tools];

- independent audits of system security by people not directly involved in programming or system management of the audited system;

- hazard analysis evaluating threats to safety from different malfunctions and breaches of security [e.g., consequences of tampering with patient data in hospitals].

2) Take specific short-term actions now:

- Develop security policies for your organization before there's a problem;

- Form and train computer emergency response teams before a crisis to respond to security violations or attacks;

- Use the Orange Book's (TCSEC, from the National Computer Security Center's Rainbow series) C2 and B1 criteria to define guidelines on security;

- Improve software systems development by applying better quality-assurance methods;

- Contribute to voluntary industry groups developing modern security standards and implement those standards in commercial software;

- Make effective security the default in software and hardware (make the user explicitly disable security instead of having to enable it).

3) Learn and teach about security:

- Build a repository of incident data;

- Foster education in engineering secure systems, both by encouraging universities to provide post-graduate training in security and urging industry to include security training as part of software engineering projects;

- Teach beginners about security and ethics in computer usage and programming [e.g., the NCSA is working on a research and development project to study beliefs, attitudes and behavior about ethical issues in computing in grade- and high-schools, colleges, and universities].

4) Clarify export control criteria and set up a forum for arbitration [hardware and software vendors have been complaining for years that the arbitrary imposition of severe export restrictions hampers American competitiveness in overseas markets without materially helping national security].

5) Fund and pursue needed research in such areas as

- security modularity: the effects on security of combining modules with known security properties;

- security policy models: more subtle requirements like integrity and availability are still not easily represented by control structures;

- cost estimation: there should be better ways of measuring the costs and benefits of security mechanisms in particular applications;

- new technology: networking, in particular, leads to greater complexity (e.g., how to connect ‘mutually suspicious organizations’);

- quality assurance for security: how to measure effectiveness;

- modeling tools: standards for graphical representations of security relationships analogous to the diagrams used in functional decomposition and object-oriented methodologies for program design;

- automated procedures: audit and monitoring tools for the data center management team;

- nonrepudiation: combining the need for detailed records of user actions with the values of privacy;

- resource control: how to ensure that proprietary software and data are used legitimately (e.g., preventing more than the licensed number of users from accessing a system, preventing software theft);

- security perimeters: how to reconcile the desire for network interconnection with limitations due to security requirements ('If, for example, a network permits mail but not directory services... less mail may be sent because no capability exists to look up the address of a recipient').

Chapter 2 of the NRC report, 'Concepts of Information Security,' is a 25-page primer on information systems security that could be handed to any manager who needs to be filled in on why you propose to spend so much money protecting the computer systems. The authors cover the fundamental aspects of information security (confidentiality, integrity and availability); management controls (individual accountability, auditing and separation of duties); risks (probabilities of attack or damage) and vulnerabilities (weak points); and privacy issues. In Appendix 2.2, the authors report an informal survey in April 1989 of 30 private companies in a variety of fields. The consensus among those polled included the following basic standards for information systems security (show these to your upper management if necessary):

- unique IDs, block access after a maximum number of incorrect logon attempts, show last successful access at logon time, make passwords and IDs expire;

- disallow embedded passwords during logon, make passwords invisible during entry, force minimum length (6), store passwords encrypted, scan proposed passwords to eliminate easy words;

- permit strict control over file access;

- detect and interdict viruses, certify software as virus-free, provide data encryption, overwrite deleted files to prevent recovery, force tight binding of production data to production programs;

- automated time-out for inactive sessions, unique identification of terminals/workstations during logon;

- network security monitoring, modem-locking, callback, automatic data encryption during transmission;

- audit trails including security violations;

- generally applicable security standards that could be used by vendors and users to evaluate different equipment and software for specific environments.

History

We live in a society so permeated with information technology that we forget that computation, tallying, and communication were once the domains of tiny elites. Entire civilizations rose and fell with a fraction of the information processing power we take for granted. Getting news from one end of the Roman empire to the other could take weeks; simple multiplication using Roman numbering required specialized training. However, despite the complexity of modern information processing, very little in modern information systems security would have been incomprehensible to an educated person from hundreds or even thousands of years ago.

Enterprise systems security is primarily a question of human behavior. The specifics of protecting specific equipment and programs are details of implementation. If people don't care about security, even the most sophisticated and expensive security mechanisms will be wasted. The Post-It(R) sticky note is probably a greater threat to security in your organization than the teenaged cracker lusting to crack your access codes.

Throughout history, people have protected information against unwanted disclosure. Documents have been locked away — an early form of access control. Julius Caesar is said to have encoded secret documents by translating each letter to the one a fixed distance ahead in the alphabet — a monoalphabetic cipher. Writers and inventors created secret languages to protect themselves against persecution and theft.

Computing machinery has changed in form and power over the millennia. Concerns over security have changed as a result. About 5000 years ago, the Babylonian abacus was the pocket calculator of the time; security centered around protecting the device from theft and destruction.

In 1614, John Napier invented logarithms. For centuries, scientists and engineers depended on logarithmic tables for multiplications, divisions, powers and roots. Errors in these tables could cause severe failures. Security centered around accuracy.

William Oughtred's slide rule was as revolutionary in its day as the abacus and the pocket calculator were in their times. Physical protection and quality control during production were critical security concerns.

Physical security was paramount through the ages of the digital adding machine of Blaise Pascal (1642), Wilhelm Leibnitz' hand-cranked calculator (1673), the Jacquard Loom (1804) with its punched cards and Herman Hollerith's punch-card tabulator and sorter (1890). Owners of these expensive machines were primarily concerned with protecting them against damage and malfunction.

During the decades from 1930 to 1950, computing machinery was expensive and rare. Each model was unique: Vannevar Bush's Differential Analyzer (1930); George Philbrick's analog computer, Polyphemus; Bell Laboratories' Complex Number Calculator (1940); the Rockefeller Differential Analyzer (1942); Colossus (1943), with its 2000 vacuum tubes. The Harvard Mark I (1944), was fifty-one feet long and had a speed of 3 adds per second; it was used for 16 years to calculate ballistics tables for the U.S. Navy. ENIAC (1946) filled a room. In the early 1950s, it

was commonly assumed that computers would never be widespread; after all, who but governments and a few large corporations could afford something as expensive as UNIVAC?

By the 1960s, the ‘glass house’ was the norm. Large computers were placed in glass-walled enclosures where proud executives could show them to visitors. Security still focussed on the physical parameters. Giant processors required adequate cooling, including cold water flowing through the equipment and air conditioners for the rooms filled with tape drives. Electrical power quality rose in importance; computer centre managers installed isolation transformers and uninterruptible power supplies. Cipher locks became the norm for controlling access to the hardware.

As data processing shifted towards information processing in the 1970s, data centre managers invested in logical access controls. The widespread use of multiple-user operating systems naturally led to concern over privacy and protection of each user's information. For example, the MULTICS project at MIT in the mid 1960s included multi-level security that would allow Top Secret, Secret, Confidential and Unclassified data to reside safely on the same computer. UNIX is an offshoot of MULTICS; by the mid 1970s, it included powerful mechanisms for protecting files, memory structures, and system resources. Other proprietary operating systems (e.g., those for IBM mainframes and Digital Equipment Corporation's and Hewlett-Packard's midrange systems) also include extensive security mechanisms for file and system protection.

Remote computing started with the American Mathematical Society's meeting at Dartmouth College. On September 11, George R. Stibitz used a teletype link from Hanover, New Hampshire to the Complex Number Calculator at Bell Labs' offices in New York City to transmit problems and receive answers. Dartmouth College was also a pioneer in public time-sharing, with its student- and faculty written Dartmouth Time-Sharing System (DTSS) operating system for General Electric and Honeywell computers. By 1967, DTSS was supporting dozens of remote terminals, some of them linked by phone lines using modems. With the growth of networking came concerns over unauthorized listening (eavesdropping) and undetected modifications of the data stream.

The first microcomputers widely used in business were the IBM PCs, introduced in 1981. The introduction of the PC complicated security for managers who had become accustomed to centralized controls. Users and departments sometimes became rogue computer centers, functioning with non-standard hardware, software and procedures. Naive users knew nothing about backups and passwords; they left their systems open to intrusion without even thinking about corporate information. Disaster plans failed to include microcomputers, even though an increasing share of corporate information actually resided on little hard and floppy disks.

As distributed computing environments spread through the 1980s, new security challenges faced the growing number of local information systems managers. Local area networks were notoriously unstable, with periodic destruction of individual records, files or entire disk volumes. Untrained staff were assigned to do backups — and never thought to verify that their tapes and cartridges were actually readable. Concerns over privacy grew as governments, third-party data vendors and employers collected and shared information about more and more of the population. Computer foul-ups caused ever-greater consequences for organizations and individuals.

Now, in the mid 1990s, 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 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

The classic definition of information security is drawn from IBM Corporate Policy Number 130, as quoted in Carl B. Jackson's 1992 paper, ‘The need for security’ (see chapter notes).

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 (affectionately known as the 'Bald Eagle of Security'), a respected author, teacher and thinker in the security field and a principal in the SRI high-tech consultancy , has added to these possession, authenticity and utility.

Definitions

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 security

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.

The problem of ascertainment

The difficulty in describing the risk of facing these threats is that we lack proper statistical information about how often different types of damage occur. In statistical work, this difficulty is known as the problem of ascertainment. Most organizations are reluctant to admit, let alone publicize, successful attacks on their information systems. Would you be comfortable putting your money in a local bank after it revealed a million-dollar fraud? Would you use a law firm whose client records had been used for blackmail?

The second part of the ascertainment problem is that even if people were reporting all the computer crimes and accidents they knew about, we would still not know about the crimes and accidents that have not yet been discovered.

You should therefore doubt the accuracy of all statistics about the incidence of damage and threats to information systems.

Having said all that, we still have to explain to managers and others why we want to spend their money on security. The following graph shows rough guesses about the causes of damage to information systems. Think of it as a guide to the industry consensus.

<<insert Figure 1-1>>

As you can see, the most significant cause of damage is ignorance and carelessness. Fire is a serious threat; water damage often accompanies fires because of fire-suppression systems and fire fighters. Unhappy and dishonest employees account for most of the rest of the damage, with viruses a distant last (and currently only for microcomputers). Outsiders are thought to account for no more than a sixth or so of all damage to information systems.

As usual, Donn Parker has a provocative and original view of these estimates. In a 1990 paper, he argued that, among other points,

- We don't know how much these attacks cost or many there are;
- We don't know what proportion of human threats are caused by outsiders;
- Most computer criminals are not so much greedy as unhappy or desperate;
- Computer viruses are still a negligible threat;
- Information stored in computer systems is safer than voice and print;
- Electronic eavesdropping is discussed by security experts because it is interesting, not because it happens;
- Computerization decreases business crime;
- Business security should emphasize the need-to-withhold, not the need-to-know.

Threats from insiders

Despite our qualms about ascertainment, there are nevertheless surveys which give us some idea of the situation. In 1984, for example, the American Bar Association Report of Computer Crime

suggested that about 78% of all offenders in computer crimes were insiders who usually had authorized access to the systems they damaged or abused.

Disgruntled employees are the third most costly threat to information systems (after fire and water). This finding supports the view that management supervision and sensitivity to mood and morale are crucial foundations for effective security.

Unionization is an interesting question. In my own practice, I was asked by a manufacturing firm to serve as an expert witness in a planned court case. The employer wanted to oppose unionization of its computer operations staff. They felt that unionized employees would pose a threat were there ever a strike by the rest of the employees. The funds set aside for the legal battle were more than $100,000 (in 1986). I asked, ‘How do we know that unionization is bad for security?’ Accordingly, the company commissioned me to search the published literature for references to unionization and security.

There were 39 articles from the previous decade which dealt with the issue. Thirty-seven argued that, far from decreasing security, unionization could actually improve computer room security. Unionized employees were more willing than non-union staff to follow detailed, written security procedures. Detailed access control audit trails based on electronic card readers were more acceptable than to some non-union staff. The company saved its $100,000, much to the displeasure of its lawyers.

Threats from outsiders

Outsiders are still an over-rated threat, but that threat may increase. Amateur criminal hackers are a minor problem, despite overblown media reporting. However, organized crime has a serious interest in personal information and computerized access to the monetary system. In addition, today's highly-competitive international market makes industrial espionage attractive to unscrupulous clients and lucrative to information thieves.

Computer criminals run some of the world's most highly secured systems: underground bulletin board systems (BBSs). Unlike the majority of BBSs, which are run by and for innocent cyberspace enthusiasts, criminal BBSs store and provide dangerous information about interesting victims — especially large, high-tech companies and financial institutions. In private areas restricted to those who have provided illegally-obtained information, these BBSs supply browsers with dial-up port telephone numbers, stolen telephone credit card numbers and bank credit card details. Some companies monitor these BBSs to keep track of their own vulnerabilities. For example, a school commission in Montreal found its dialup numbers and logon procedures in a local BBS.

Statistics

In a 1992 survey, USA Research, Inc. estimated about 700,000 cracker attacks per year in the United States. They calculated that there was a 1 to 2% probability that a given computer system would be attacked in any given year, and that the total damage (in lost productivity or sales) caused by criminal hackers was about $150 million in 1991.

Another area of growing abuse is phone fraud. Criminals steal phone services and resell them for enormous profits. James Snyder, Special Counsel for Investigations at MCI Telecommunications Corporation, addressed the Tele-Communications Association (TCA) 1992 Annual Conference in San Diego in September 1992. He warned that organized crime has found selling stolen phone services to be highly profitable and low in risk. Stolen access codes are being sold to other criminals for prices ranging from $3,000 to $10,000. According to Detective Don Delaney of the New York State Police, some thieves are earning more than $1M annually through call resell operations.

Lawrence Gessini, Director of the International Communications Association, addressed a special hearing of the Federal Communications Commission (FCC) in October 1992. His members reported theft of phone services amounting to $73.5 million over three years. The losses occurred in 550 cracker attacks on Customer Premise Equipment (CPE), including Private Branch Exchanges (PBXs), electronic Voice Mail Systems (VMSs), and Automated Call Distributors (ACDs).

In a recent DROIS report, Ira Herzoff estimates telecommunications losses an order of magnitude higher: $3M a day and annual losses in the $1B to $2B range.

Information systems managers must either work closely with managers responsible for telecommunications equipment or must consolidate voice processing with data processing into an integrated enterprise information systems directorate. It is no longer possible to consider information security without including voice systems.

Information warfare

Threats to information systems have largely been from accidents, as discussed above. However, for some organizations, the threats may change. The rise of global competition suggests that we are entering an age of *information warfare.*

Historical perspective

Throughout the history of conflict, technology has provided both weapon and target. When warriors mounted horses, their steeds provided both threat and vulnerability to opponents. To harm a single mounted man, one could attack his horse. To imperil a nation of horsemen, one could poison the herds. Armored knights fell to crossbows, but a more subtle attack was to destroy the foundries.

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.

Cultures that depend on information systems are vulnerable to information warfare. Information warfare consists of deliberate attacks on data confidentiality and possession, integrity and authenticity, and availability and utility. Information warfare can harm individuals, corporations and other private organizations, government departments and agencies, nation-states and supranational bodies. Information warfare is the extension of war into and through cyberspace. Military planners have recognized their dependence on information technology; some forces now speak of C4I: Command, Control, Communications, Computers and Intelligence. Protecting the technology of war against attack is an obvious extension of the military mind set; smart bombs require smart defenses. However, there is still no general agreement within the military establishments of the planet on the importance of protecting civilian as well as military information infrastructure. As for civil defense, there is a long way to go in including the information infrastructure as a necessary component of protection and recovery operations. Federal government departments are at least required to pay attention to the Government Security Policy, which mandates attention to security and business resumption planning (BRP); however, the task has barely begun in most departments. Provincial and municipal governments are at different stages of awareness and implementation of security and BRP. Finally, in the civilian arena, there are still many organizations which assume that disasters — let alone deliberate attack — will never strike.

Given the degree of dependence on information systems, it is essential to erect legal, organizational, and cultural defenses against information warfare.

Conceptual framework

Winn Schwartau 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.

The possibility that organizations will be the target of deliberate attack profoundly alters the process of *risk assessment*, which is the subject of the next section of this chapter.

Risk assessment

Most adults realize that insurance is a balance between costs and risks. We decide that the cost and inconvenience of replacing the oil in our car is minor compared with the consequences of dirty or insufficient oil. We pay insurance companies to protect our investments in houses and cars. Cellists insure their hands but not their lips; flautists insure their lips but not their hands. We have to know how much an asset is worth to us and then estimate the risks to that asset before we can make rational decisions about how much effort to expend in protecting the asset.

As in daily life, so in enterprise security. You cannot reasonably develop security policies and procedures without having a clear idea of the systems you want to protect and how valuable they are to you. In addition, you have to determine — or more usually, guess — the probability that your assets will be threatened.

Critical and sensitive data

There are two dimensions by which you have to measure the value of your information assets.

Critical information must be available and correct for your operations to continue at acceptable levels of efficiency and effectiveness. For example, in a hospital, clinical data provided at the bedside to treating physicians and nursing staff are critical: unavailability or inaccuracy may threaten people's health and even their lives. On the other hand, the hospital's internal newsletter, although valuable, is not critical.

Data have different degrees of criticality. Time, for instance, can make data less critical. Last week's backups are not as critical as yesterday's backups. Accounting data from five years ago may be important in case of an audit, but they are not as critical as this year's financial figures.

Sensitive information must be protected against unwarranted disclosure. A simple way of thinking about sensitivity is to ask whether you would be comfortable seeing specific information

- Only in a private memorandum to your boss;
- In a memo to your peers;
- In a memo only to the people you supervise;
- In a company internal newsletter;

- In the stockholders' annual report;
- On the evening television news.

Continuing our hospital example, a patient's age is less sensitive or confidential than the results of a test for Human Immunodeficiency Virus (HIV). Both data are more sensitive than an in-patient's room number in the hospital.

Quantitative risk analysis

Risk analysis is the process of developing a risk assessment. The assessment is a report showing assets, vulnerabilities, likelihood of damage, estimates of the costs of recovery, summaries of possible protection and costs, and estimated probable savings from better protection.

There are two broad classes of methodology for risk analysis: quantitative modeling and qualitative estimating. Quantitative risk analysis developed first, in the 1970s. It uses numerical estimates of cost and probability to generate models of expected loss and expected savings. There are many software packages available to aid users in developing such models, most have different assumptions and algorithms and produce risk assessments that differ in their details.

Qualitative risk analysis developed because of criticism that the quantitative methods were based on illusory precision. Qualitative methods explicitly use subjective judgement scales; e.g., severity ratings expressed as ranks from 1 to 10. The arguments over methodology obscure the fundamental uncertainty of all risk estimates. As Charles Pfleeger has pointed out in his university text on information systems security, ‘The precision of numbers is a red herring. Risk analysis is best used as a planning tool.’ He emphasizes that all risk assessments should be used to point out areas of greatest concern; haggling over precise numbers is a waste of time.

Systematic risk analysis begins with a tabulation of enterprise assets. Although you can restrict this tabulation to information systems only, many analysts extend the process to cover global assets. In many organizations, this tabulation may be the first opportunity to develop a view of how much you depend on your information systems. Information systems assets include equipment, programs, data, documentation, supplies and staff. Investment in acquisition, development and maintenance of information systems have been studied by the staff of Computerworld for many years; the annual Premier 100 reports published in September list information systems expenditures as percentages of total revenue. Dun & Bradstreet Corporation, for example, was estimated in 1992 to have spent over 16% of its gross revenue on information technology. On average, the best users of computer systems spend 1% to 5% of their annual revenue on their information systems.

For each asset, you must brainstorm to imagine as many risks as you can. Look at physical damage, errors, criminal behavior by employees and other insiders, and breaches of security by outsiders. List the potential effects of compromising confidentiality, data integrity and system availability. Imagine the effects of unavailability for an hour, a day, a week. For example, a factory that uses computerized bar-code readers to keep track of production may continue operating for an hour or two if the bar-code reader system fails. However, it may shut down completely if the systems are unavailable for a day or more. Think of a university whose registration system depends on computer databases. Errors or accidents that delay registration for more than a week may cause serious problems for students and staff. Failure of a clinical information system for longer than minutes could put patients at risk of injury or death; it could also put doctors at risk of malpractice suits and the hospital administrators at risk of prosecution for negligence.

The preliminary study may lead to better awareness of security issues among your staff. One of the most important contributions of risk analysis to better security is that every employee can contribute insights. The people best positioned to evaluate risks and consequences are those who use the tools under evaluation.

Another advantage of undertaking such a study is that it is the basis not only of improved security policies and procedures, but it also serves as the first step in disaster prevention, mitigation and recovery planning.

The hardest part of quantitative risk analysis is estimating probabilities. Actuarial data compiled by insurance companies can help you estimate risks; however, all such general figures must be taken as guides, not eternal truths. The probability of loss is strongly influenced by your own situation. For example, the risk of water damage may be (say) 1% per year in general — but if your buildings are located near a badly-constructed dam, your probability is higher than average by an unknown amount.

Recently, spreadsheet add-in packages have appeared to help model risk using appropriate probability distributions. These tools allow risk managers to apply Monte Carlo simulation techniques, in which the probability of complex events is estimated by repeated sampling of more elementary components linked in a causal chain.

Some risk analysis packages include extensive databases of actuarial data and expert knowledge about different industries. You can install modules dealing with banking, manufacturing, insurance, federal and state governments, physical security, microcomputers, telecommunications, computer applications, and disaster recovery. Costs of such packages range from less than $100 per copy into the $20,000 range. The more expensive packages use artificial intelligence techniques, including fuzzy logic, to model your risks, costs of counter measures, and annualized savings. The sophistication of reports is also correlated with cost; the more costly packages provide several levels of reporting (e.g., executive summary and decision support with graphics and tabular details in the technical analyses). Because the field continues to evolve, you should consult reviews in DROIS and in the technical press before choosing a specific package.

Qualitative risk analysis

Many of the risk analysis packages include qualitative measures. However valuable, these models nonetheless provide less support for the monetary estimates that managers have come to expect from their information systems staff. It is ironic that many people would rather have bad estimates expressed as dollar figures than better estimates couched in qualitative terms.

Risk analysis in the age of information warfare

Threat and risk assessment has traditionally dealt with the probability of Acts of God. Fire, flood, earthquake, even burglary can be looked at as involving random events. However, in today's competitive and unethical environment, the likelihood of being attacked is an unknown and unknowable function of an organization's attractiveness and preparedness. The most successful and least secure organizations will be victim. Faced with a choice between an unkempt hovel and a palatial residence, a thief will try to rob the more lucrative target. But suppose a thief sees two palatial residences: one has Doberperson Pinchpersons (politically correct guard dogs) roaming the space inside a 3 meter fence, infrared motion detectors and a direct link to a security company; the other has locks on the doors. There's not much doubt about the selected victim.

In my courses, I like to explain the principle of appropriate defense with a story. Two hikers are walking happily along a trail in Alberta when they come upon a huge grizzly bear. Turning tail, they being running down the trail. One huffs to the other, "This is (pant, gasp) crazy. We can't outrun a grizzly bear! They can run 30 km an hour and climb trees!@ The other gasps, "I don't have to outrun the grizzly bear (pant, pant). I just have to outrun *you.*"

To pursue the analogy, unprepared organizations may be in the position of hikers unaware that they are covered in honey when there are bears on the path. Risk assessment in the age of information warfare must include self-examination from the point of view of a competitor. Organizations must recognize when they are attractive to predators and must then make themselves unattractive targets for espionage and sabotage.

Summary

The pervasive use of information technology in the developed world has brought with it a widening need for security. Information security includes concerns for protecting information assets from unauthorized or accidental modification and disclosure. Security includes the need for preserving confidentiality, integrity, availability, utility and authenticity. Because of under-reporting of computer crime, we should mistrust statistics about attacks and accidents that damage information. The consensus is that the most serious risks to information systems come from authorized personnel who are either inadequately trained, inattentive, angry or dishonest. Criminal hackers and viruses are significant but over-rated threats. Information security policy development must begin with a thoroughgoing analysis of sensitivity and criticality. Risk analysis software can bring artificial intelligence and industry expertise to bear on the production of detailed risk assessments. Human factors make risk analysis more difficult in the age of information warfare.

CHAPTER NOTES

These notes represent details of where to look for more information. Since this text is not intended as a scholarly review of the field, but rather as a guide for practitioners, I have not interrupted the flow of your reading by inserting numbered footnotes or endnotes. The notation v(n):p (as in PC-Computing, 3(8):122) means volume v, number n, page p (thus volume 3, number 8, page 122 and following). As much as possible, I have restricted the choice to readings from 1990-1995.

1. System Security Study Committee, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, National Research Council (1991). *Computers at Risk: Safe Computing in the Information Age.* National Academy Press (2101 Constitution Ave NW, Washington, DC 20418). ISBN 0-309-04388-3 (paper). xv + 303 pp. Bibliography, appendices. Also available from the National Computer Security Association (NCSA).

2. National Computer Security Center (NCSC). The "Rainbow Series" includes (among other titles):

   Orange Trusted Computer System Evaluation Criteria

Red	Trusted Network Interpretation
Light Green	Password Management Guide
Dark Green	Glossary of Computer Security Terms
Dark Blue	Magnetic Remanence Security Guidelines

   Yellow Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments

3. One of the most important services available for the information systems security professional is *Datapro Reports on Information Security* (DROIS). These reports, updated monthly, are an invaluable source of up-to-date information. Three large binders contain over a thousand pages of clear, detailed reports from journals, conferences and books. Many reports are especially written for DROIS and are unavailable elsewhere. You can reach Datapro Research Group at 1-800-928-2776 in the US and 1-416-298-1177 in Canada. Headquarters: 600 Delran Parkway, Box 1066, Delran, NJ 08075. DROIS is now available on CD-ROM.

4. There is a continuing debate in the technical community about whether it's too late to salvage the word *hacker* now that the popular press has demonized it. As a 15 year old learning assembler in 1965, I would have qualified as a *hacker* in the honorable sense of the word. We techno-nerds would never have sunk so low as to be *criminal hackers.* One of the terms being tossed around the Internet to describe criminal hackers include *cockroach,* which suggests the contempt in which these creeps are held by honest people.

Personally, I feel that the cockroach has a long history on the planet and that its name should not be so besmirched.

5. Many of the references in this and subsequent chapters were found through the *Computer Database Plus* offered by Ziff Communications Company through the CompuServe value-added network. This bibliographic database includes over 530,000 references to the computer trade press. More than two-thirds are *full text* articles. Costs are modest: $0.25/minute connect time, $2.50 for each full-text article downloaded, $1.50 for articles that have no abstract, and $1.00 per abstract.

   The breakdown of articles indexed by date is as follows:

   1994: 76,557
   1993 73,680
   1992: 83,148
   1991: 78,705
   1990: 68,979
   1989: 62,029
   1988: 47,405
   1987: 33,580

   Selection criteria permit Boolean operators (AND, OR, NOT) in several fields including:
   Key Words (words in article titles, subject headings, company or product names)
   Subject Headings (including lookup and menu functions)
   Company Names
   Product Names
   Publication Names (including a list of all publications and their addresses)
   Publication Dates (1987 to present)
   Article Types (e.g., opinion, tutorial, buyers' guide)
   Words in Article Text.

   Lookups rarely take more than a few seconds. The number of hits is shown and a menu of article titles of possible interest is available for inspection. Specific articles can then be read or downloaded.

   Everyone who joins the National Computer Security Association receives a free CompuServe membership kit and can participate in the NCSA security section.

6 Excellent overviews of computer crime and security (listed from most recent to oldest):

Flaherty, F. (1994). Cyberspace swindles: old scams, new twists. *New York Times* 143(July 16, 1994):25

Kelly, S. (1995). Highway to Hell? *Computer Weekly* (March 2, 1995):30

Coffee, P. (1994). Developers must guard against fraud, snoopers. *PC Week* 11(30):1

Newsome, C. (1994). Data security threat as crime increases. *PC User* (246):14

Jackson, C. B. (1992). The need for security. DROIS report #IS09-100-101. This report contains a wealth of valuable insight and details of practical implementation.

Herzoff, I. (1992). Voice network fraud. DROIS report #IS35-200-101. Mr Herzoff provides the address of the Communications Fraud Control Association / 2033 M Street NW / Washington, DC 20036; tel. 202-296-3225.

Snyder, J. F. (1992). Toll fraud today. *Proceedings* of the 1992 Annual Conference, Tele-Communications Association; San Diego, 21-25 Sept. P. 415.

USA Research, Inc. (1992). *IPA Computer Virus and Hacker Study*. 4 volumes, 300 pp. USA Research, Inc. / Technology Company Information Reports / 4380 SW Macadam Avenue / Portland, OR 97201-6406 / Tel. 503-274-6200 / Fax 503-274-6265.

NCSA (1991). *Computer Virus Prevalence Study*. Available from the National Computer Security Association.

Parker, D. B. (1991). Restating the foundation of information security. Paper presented at the 14th National Computer Security Conference in Washington, D.C. (October 1991). Reprinted as DROIS report #IS09-125-101. This paper lays out Parker's thoroughgoing revision of the classic goals of information security.

Parker, D. B. (1990). Seventeen information security myths debunked. *ISSA Access* 3(1):43. Reprinted as 'Information myths explained,' in DROIS report #IS09-150-101.

Manning, R., D. Pearlman, & D. Steinberg (1990). To catch a hacker. *PC-Computing* 3(8):122.

7 Risk analysis software

Classe, A. (1994). Hazard warning. *Computer Weekly* (Nov 17, 1994):56

Waring, B. (1994). Crystal Ball 3.0: Excel add-in provides intelligent risk analysis. *MacUser* 10(10):64

Duncan, R. J. (1992). Risk analysis software: overview. DROIS #IS21-001-101. This report includes detailed comparisons of 13 packages, including general information about the product and its sales, host requirements, source code, operation, risk analysis features, report generations, support and prices.

Ozier, W. (1992). Issues in quantitative versus qualitative risk analysis. DROIS #IS20-250-101. Will Ozier summarizes the metrics available for both approaches to risk analysis.

Pfleeger, C. P. (1991). Security in Computing. Prentice-Hall (Englewood Cliffs, NJ). ISBN 0-13-798943-1. Chapter 13, pp. 457-470, includes several examples of quantitative risk analysis.

8 On information warfare:

Kabay, M. E. (1995). M. E. Kabay on Information Warfare. *Computerworld* 29(12):48 (insert)

Schwartau, W. (1994). *Information Warfare: Chaos on the Electronic Superhighway*. Thunder's Mouth Press, New York. ISBN 1-56025-080-1. 432. Index.

9 The NCSA Forum on CompuServe [now defunct] provides an excellent opportunity for professional discussion of information security issues with security experts and other managers and users of computer systems. As of May 1995, there were over 29,000 participants in the Forum.

Sections include

1	About NCSA	Information about the Association; NCSA events
2	Ethics/Privacy	Protecting personal information in cyberspace; policy issues such as censorship, anonymity
3	News/Case Studies	Security events, computer crimes, fraud using computers
4	Anti-Virus Support	News of recent outbreaks, support in diagnosis of virus attacks and damage repair
5	Disaster Recovery	Disaster prevention, mitigation, and recovery planning; postings from Internet newsgroups dealing with natural disasters; discussions of quality assurance failures in software and hardware
6	Encryption	Technical, policy, and regulatory issues involving encryption; support for PGP users; front-ends for encryption packages
7	PL/MAC/LAN	Access control policies and techniques; logging; software license compliance; network monitoring
8	UNIX/Internet	Firewalls, bug reports, fixes
9	Telco Security	Toll fraud, voice mail, fax security
10	Crime/Law/Policy	Legal initiatives, statutes; corporate policies
11	Electronic Commerce	Electronic data interchange, funds transfers
12	Host/Single Signon	Large system security; RACF, ACF/2
13	Product Info/PR	Infosec product descriptions, press releases
15	Auditing	Systems auditing, log files, quality assurance.
16	Certification/Training	Professionalization, education, teaching
17	BBS/Sysop	Security for bulletin board system operators
18	UNCLASSIFIED	Friendly area for casual discussions
19	Book Reviews	The latest security books

20	Special Topics	Recently set aside for Pentium Bug; available for other hot topics as required
21	Electronic Seminar	Interactive seminars on security
22	Security Management	American Society for Industrial Security (ASIS) area
23	PRISM Members Only	Reserved area for subscribers to special NCSA services

<<end of chapter>>