January 1989

Curb on Technology: Liability for Failure to Protect Computerized Data Against Unauthorized Access

Michael H. Agranoff

Follow this and additional works at: http://digitalcommons.law.scu.edu/chtlj

Part of the Law Commons

Recommended Citation
Available at: http://digitalcommons.law.scu.edu/chtlj/vol5/iss2/3

This Article is brought to you for free and open access by the Journals at Santa Clara Law Digital Commons. It has been accepted for inclusion in Santa Clara High Technology Law Journal by an authorized administrator of Santa Clara Law Digital Commons. For more information, please contact sculawlibrarian@gmail.com.
CURB ON TECHNOLOGY: LIABILITY FOR FAILURE TO PROTECT COMPUTERIZED DATA AGAINST UNAUTHORIZED ACCESS

Michael H. Agranoff†

TABLE OF CONTENTS

I. INTRODUCTION ...................................... 265

II. UNAUTHORIZED ACCESS TO DATA: HARM, LIABILITY, AND STANDARDS OF DUE CARE ............................ 266

A. Printed Data ....................................... 266
B. Computerized Data ................................ 267
C. Liability for Third-Party Actions ............... 268
D. Standards of Care in Various Situations .......... 269
   1. Law Office Case ................................ 269
   2. Hospital Case ................................ 271
   3. Service Bureau Case ......................... 271
   4. Additional Examples .......................... 272
E. General Standards of Care ....................... 274
   1. Lack of Generally-Accepted Standards ....... 274
   2. Consequences of Lack of Standards ........ 275

III. COMPUTER SECURITY DEMYSTIFIED: IDENTIFYING PROBLEMS OF "DUE CARE" IN THE PROTECTION OF COMPUTERIZED DATA ........................................ 276

A. The Need for Understanding ...................... 276

Copyright © 1989 Michael H. Agranoff. All Rights Reserved.

† B.A., magna cum laude, University of Hartford, 1968. J.D., magna cum laude, University of Connecticut, 1988. Member of the Connecticut Bar. Currently, an associate with John C. Peters & Associates, West Hartford, CT 06107. The author has nearly 20 years experience in large-scale computer data processing with a major financial institution; including nearly 10 years in computer security, with administrative implementation and technical liaison for several online countrywide computer security software systems. The author has published several articles in trade journals and given workshops at national and local trade organizations.

1. The author wishes to acknowledge with deepest appreciation the assistance of Professor Dennis Stone of the University of Connecticut School of Law. Professor Stone acted as advisor to the author for two years in the research project which became the basis of this paper.

The author would also like to thank Professor Loftus E. Becker, Attorney Jay Bloom Becker, Dr. Willis H. Ware and Dr. James Burrows for their assistance and helpful comments; and Attorney John C. Peters for his encouragement and belief in this endeavor.

263
B. Functional Elements of a Computer System .. 278

C. Basic Elements of Computer Security .......... 282
   1. Note on Data Exposures ..................... 282
   2. Categories of Controls ...................... 284
      a. Physical Security Controls .......... 284
      b. Access Control Software ........ 285
      c. Dial-Up Controls .................. 285
      d. Encryption .......................... 287
      e. Administrative Controls ........ 287

D. Access Control Software Models .............. 288
   1. Identification .......................... 288
   2. Authentication .......................... 289
   3. Authorization ........................... 291
   4. Logging .................................. 294
   5. Monitoring and Surveillance ............. 294

E. Selected Problems in Computer Security
   Implementation ................................ 295
   1. Proving Identity ........................ 295
   2. Restricting File Access .................... 299
      a. Sensitive Residue .................... 299
      b. Bypass Mechanisms .................. 300
      c. Lack of Uniform Security Architecture 303
   3. Ensuring Individual Privacy in Statistical
      Data Banks .............................. 304
   4. Miscellaneous Issues ...................... 306
      a. Electronic Mail ...................... 307
      b. Violation Reporting .................. 307
      c. Administrative Methods ............ 308

IV. PROTECTION OF SOCIETY: THE NEED FOR
    MEANINGFUL FEDERAL COMPUTER SECURITY

    A. Differing Views on Developing Standards ...... 310
    B. Response of the Organized Bar ................ 312
    C. Corporate Management Response ............. 313
    D. Congressional Response .................... 313
       1. The Recognition ....................... 313
       2. The Promise: The Computer Security Act of
          1987 .................................. 315
       3. The Prospects .......................... 317

V. CONCLUSION ..................................... 319
CURB ON TECHNOLOGY: LIABILITY FOR FAILURE TO PROTECT COMPUTERIZED DATA AGAINST UNAUTHORIZED ACCESS²

I. INTRODUCTION

Reliance upon computers in modern society has caused a greater awareness of the problems that can result from unauthorized computer access³ and abuse. Despite this awareness, however, no standards presently exist which specify the precise degree of computer security⁴ required to prevent liability. The result is that

2. "The central storage and easy accessibility of computerized data vastly increases the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology." Whalen v. Roe, 429 U.S. 589, 607, 97 S. Ct. 869, 880 (1977) (Brennan, J., concurring).

3. "Access" in the broadest sense refers to one's ability to use a computer system. In a narrower sense, however, it refers to one's ability to affect a particular data item on a computerized file. The term, as used in this article, means the ability to read, modify, or destroy a specific data item. Therefore, unauthorized access, with respect to a specific data item on a computerized file means the fact of reading, modifying, or destroying that data item in an impermissible manner.

4. The standard definition of "data security" is the "protection of data against accidental or intentional disclosure to unauthorized persons, or unauthorized modifications or destruction." J. MARTIN, SECURITY, ACCURACY, AND PRIVACY IN COMPUTER SYSTEMS 5 (1973) [hereinafter Martin]. See also R. FISHER, INFORMATION SYSTEMS SECURITY 20 (1984) [hereinafter Fisher]. "Computer security" is "the technological safeguards and managerial procedures which can be applied to computer. . .data to assure that organizational assets and individual privacy are protected." L. HOFFMAN, MODERN METHODS FOR COMPUTER SECURITY AND PRIVACY (1977) [hereinafter Hoffman].

Violations of computer security are often termed "computer abuse." It is important to understand that there are many types of computer abuse other than unauthorized access. For example, the most perfect protection against unauthorized access will not stop authorized individuals from acts such as fraudulently altering records, selling proprietary data to competitors, using the company's computers to run their own business, or taking illegal advantage of confidential computerized information. See generally, A. BEQUAI, HOW TO PREVENT COMPUTER CRIME 17-21 (1983) [hereinafter Bequai].

Further, computer negligence can involve many things other than security. We shall not deal with product liability for software, (See, e.g., Gemignani, Product Liability and Software, 8 Rutgers Computer & Tech. L.J. 173 (1981); Conley, Tort Theories of Recovery Against Vendors of Defective Software, 13 Rutgers Computer & Tech. L.J. 1 (1987); Reece, Defective Expert Systems Raise Personal Injury Liability Issues, Nat'l. L.J., Oct. 12, 1987, at 24-29 (inevitable that courts will have to address theories of liability as persons are injured as a result of defective systems)) or with breach of warranty (See, e.g., Comment, The Warranty of Merchantability and Computer Software Contracts: A Square Peg Won't Fit in a Round Hole, 59 Wash. L. Rev. 511 (1984) (authored by Edward Durney); Raysman & Brown infra note 22, 9. 3.04 (1987); Friedman & Hildebrand, Computer Litigation: A Buyer's Theories of Liability, The Computer Law., Dec. 1987, at 34 (avoiding pro-vendor provisions of the standard hardware/software contract)). These important computer-related actions are beyond the scope of this paper and are not concerned with unauthorized access except in the most incidental manner.
victims of computer abuse are unlikely to be compensated for their misfortunes, since there is no reference point against which to measure negligence or failure to perform at accepted professional skill levels. This is an anomalous situation since general principles of computer security have been known to practitioners for over a decade.

This article seeks to explain (1) the need for establishing standards for protecting computerized data, (2) the computer industry’s reluctance to create industry-wide security measures, and (3) lawyers’ concerns in establishing standards for a still evolving industry. Section II explains in simplified terms the need for protection and highlights this need with several examples of the harm that can result from the lack of computer security. Section III attempts to familiarize the reader with general computer system fundamentals and explains the problems that routinely occur in implementing computer security. Section IV compares several views concerning the need for computer security standards and addresses the practical limitations in allowing the private sector to set security standards. Finally, this article concludes that federal regulations are needed to establish meaningful standards for implementing computer security measures and protecting against computer abuse.

II. UNAUTHORIZED ACCESS TO DATA: HARM, LIABILITY, AND STANDARDS OF DUE CARE

A. Printed Data

Unauthorized access to confidential information held by a private or public enterprise can cause a staggering amount of harm. Consider three examples. A law firm in the middle of a major case has its work product stolen, and the file falls into the hands of opposing counsel. A client’s case may be badly compromised because personal weaknesses are revealed and an attorney’s strategy is exposed. Second, radiation treatment information on cancer patients is destroyed in a fit of malicious mischief. The delay in recreating the data may cause extreme discomfort for, and threaten the lives of, several seriously ill patients. Third, a service bureau is processing tax information from a medium-sized firm to be sent to the Internal Revenue Service. Records are stolen from the bureau’s files,


and the salary of a key employee is made known to a business rival. Substantial embarrassment to the firm may result, and that key employee may be lured to the competitor by the offer of a higher salary or other benefits.

Public or private enterprises have always routinely taken steps to protect their important documents against unauthorized access. Customers and clients assume that reasonable steps will be taken to keep confidential information secure. Whether that same assumption can be made with regard to computerized data is unclear.

B. Computerized Data

In the past, confidential information was physically stored on paper kept in ordinary office files. A thief had to physically break into the files in order to gain access. Thus, enterprises were careful to invoke strong security measures to protect against such a break-in. Today, such security measures are no longer adequate. One can access confidential information in computer files without physically obtaining the data. This kind of "theft" is potentially more damaging than the physical removal of information, since computerized data can be compromised without the fact of "theft" having ever been detected.

Thus, just as customers and clients assume that a business will protect its physical files from being burglarized, they should also be able to assume that adequate computer security measures will be implemented to prevent unauthorized access to their computer files.

8. A recent work clearly expresses the present dilemma

Historically, privacy protection was augmented by cumbersome data collection and processing techniques that in themselves safeguarded individual interests. . . As long as data about medical records, credit payments, marriages. . .were kept in hard copy file cabinets in unrelated business and governmental offices, there was little chance that they could be integrated into a large information pool about the individual. Even if that had been possible, hand processing and analysis would have been prohibitive. . . . Today, exposure to uncontrolled disclosure has greatly increased. The systems that store pertinent information about individuals are accessible through small machines located in homes and operated by novices through personal telephones. . . . The personal computer, in connection with large computer systems accessible by telephone, has introduced the threat of individual voyeurism to an extent unimaginable in prior years.

C. Liability for Third-Party Actions

Suppose a person is injured by unauthorized access to personal data. To what extent is the enterprise holding the data liable for failing to secure that information. This question becomes even more important to the victim when an unauthorized accessor cannot be identified and the victim's only source of recovery is the enterprise itself.

There are several possible theories under which a victim may proceed. Generally, however, recovery is unlikely. Even if an enterprise owes a duty of care to another, it will not be liable for the tortious acts of third parties unless those acts were "reasonably foreseeable." In the past, this phrase has been narrowly construed, making it difficult for a victim to recover his loss.

Breach of contract is another alternative. An enterprise is held to the degree of skill possessed by ordinary members of that trade or business. If it fails to meet this level of care, it may be liable in contract. However, courts rarely extend protection for conduct not recognized within the professional community or expressly covered by the terms of the agreement; thus, unless an individual includes an express level of care in the contract, recovery is tenuous.

Regardless of whether liability is founded in tort or contract,

10. The act of a third person in committing an intentional tort or crime is a superseding cause of harm to another resulting therefrom, although an actor's negligent conduct created a situation which afforded an opportunity to the third person to commit such a tort or crime, unless the actor at the time of his negligent conduct realized or should have realized the likelihood that such a situation might be created, and that a third person might avail himself of the opportunity to commit such a tort or crime. RESTATEMENT (SECOND) OF TORTS § 448 (1965). See generally 57 Am. Jur. 2d Negligence §§ 206-207 (1971).
11. See Hilligoss v. Cross Cos., 304 Minn. 546, 228 N.W.2d 585 (1975) (landlord could not reasonably have foreseen that unknown thief would steal from tenant, even though landlord posted signs advertising that new apartment keys could be picked up at the building office); Irby v. St. Louis County Cab Co., 560 SW 2d 392, 396 (Mo.App. 1977) (cab company had no duty to protect decedent from intentional criminal conduct of third parties, even though it knowingly dispatched driver to a high crime area; further, "duty implied from the contractual arrangement is also limited by foreseeability. . .").
12. As a general rule, there is implied in every contract for work or services a duty to perform it skillfully, diligently, and in a workmanlike manner. With respect to the skill required of a person who is to render services, it is a well-settled rule that the standard of comparison. . .is the degree of skill, efficiency, and knowledge possessed by those of ordinary skill, competency, and standing in the particular trade or business for which he is employed. 17 Am. Jur. 2d Contracts § 371 (1964). See Graulich v. Frederic H. Berlowe & Assoc., Inc., 338 So. 2d 1109 (Fla. Dist. Ct App. 1976) and Gosselin v. Better Homes, Inc., 256 A.2d 629, 639-40 (Me. 1969).
however, it is first necessary to determine what general standards of

care are expected from businesses which hold confidential data.\textsuperscript{13} If
the injured party can prove the enterprise failed to exercise the stan-
dard of care required, he may recover. The problem is that there
are no generally accepted standards with which to ascertain the de-
gree of security required of any business. Thus, practitioners must
persuasively argue that the business failed to meet even the most
basic level of protection.

In summary, a business is not strictly liable to persons injured
as a result of unauthorized access to data. Liability depends upon
the standard of care expected from the business holding the data.
The enormous variety of computer applications in business, coupled
with powerful computer network technology, make it desirable that
modern, meaningful standards of due care exist for the protection of
computerized data against unauthorized access. With regard to the
businesses in the previous hypotheticals, let us consider the stan-
dards of care generally applied to see whether a victim might be
compensated.

D. Standards of Care in Various Situations

1. Law Office Case

Generally, a lawyer must take only reasonable precautions
against unauthorized access to files.\textsuperscript{14} If an attorney kept his
records in a safe, and a team of highly trained commandos broke
into his office and blew open the safe, he would not be liable for the
loss, since only extraordinary measures would protect against such
action.

However, suppose the attorney left his records in a washroom
and they wound up in his adversary's office. One would expect a
jury to hold the attorney liable because his actions were unreasona-
ble, and because he appears to have breached his duty of care in
failing to perform his services in an “ordinary workmanlike
manner.”\textsuperscript{15}

Although these scenarios seem extreme, there are equally ex-

\textsuperscript{13} See generally Keeton, Dobbs, Keeton, and Owen, Prosser and Keeton on
Torts 383-85 (5th ed. 1984). Even if the obligation in tort exists to control the conduct of
others, it “requires only that the defendant exercise reasonable care.” Id. at 385.

\textsuperscript{14} See generally 7 Am. Jur. 2d Attorneys At Law § 199 (1980). Even in contract, the
attorney is obliged to perform only with the degree of efficiency and knowledge possessed
by those of ordinary skill and competency within the field. 17 Am. Jur. 2d Contracts § 371
(1964).

\textsuperscript{15} Expert testimony is generally required as to the standard of care and the degree of
defendant's deviance from the standard, unless the conduct complained of is not related to
treme circumstances that might occur with regard to computer data. For example, suppose an attorney has a modern computerized law office. KGB-trained operatives, posing as carpet cleaners, install a device which captures electronic emanations from the lawyer's terminal. Whatever the lawyer types into his minicomputer is captured by the interloper. Surely the attorney would not be held liable, since only extraordinary measures could prevent such an event and KGB action is not reasonably foreseeable.

What if the situation is less clear. Assume a computer terminal is located in a law office work area which is often unattended. Taped to one side of the terminal is a piece of paper stating "JURIS" and taped to the other side is a piece of paper stating, among other things, ABC Company = 3115B. A person barely computer literate could figure out that "JURIS" is the password, and the data file number for ABC Company is 3115B. Thus, one would simply sign on using the password and request document 3115B to view strategy on the ABC Company case. In fact, one could even "steal" the data by photographing or printing it, and the attorney might not even be aware that it had been stolen.

One would expect the jury to find that the lawyer had violated due care in this situation because he failed to take reasonable precautions to prevent unauthorized access. However, the injured party would have difficulty persuading the court that the attorney failed to meet "generally-accepted industry-wide standards" since none exist with regard to computer security. Even if liability is

---

16. See PROTECTION OF COMPUTER SYSTEMS AND SOFTWARE 184-85 (F.L. Huband & R.D. Shelton, eds. 1986). [hereinafter COMPUTER SYSTEMS] (for brief technical explanation. It is true that this type of risk is generally confined to national security applications; all the more reason why a lawyer would not ordinarily be concerned with it). See also R. Kessler, Moscow Station, Time, Feb. 20, 1989 at 50, 51 (bugs implanted by KGB in Selectric type-writers at U.S. Embassy in Moscow).

17. In Practical Offset, Inc. v. Davis, 83 Ill. App. 3d 566, 404 N.E.2d 516 (1980), summary judgment for legal malpractice was affirmed against a lawyer who failed to file a financing statement necessary to perfect a security interest. The court reasoned that the lawyer's employment included responsibility for filing the statement, and that "where the record disclosed such an obvious, explicit, and undisputed breach of the attorney's duty of care, expert testimony as to the applicable standard of care would not be required. . . . It is quite possible the common sense of laymen could be relied upon to provide the requisite standard of care." 404 N.E.2d at 523 (emphasis added).

Perhaps one could also say that the lawyer's employment extends to "common sense" measures to protect client data against hackers. Query: what in laymen's common sense experience would enable them to judge the applicable standard of care needed in these technical circumstances?
found in this specific case, what precedent would be set for the less extreme situations?

2. Hospital Case

A hospital is clearly under an affirmative duty to protect its patients from physical harm by third persons. However, if one patient is injured by another, no action will lie against the hospital unless it can be shown that the risk was reasonably foreseeable. Thus, a hospital would probably be liable if it had so little security that outsiders could enter its unmanned patient records' area and wreak havoc.

Is the hospital equally charged with implementing measures to keep hackers out of its computerized patient record files? Could a jury be convinced that the risk of injury to patients is foreseeable such that counter-measures should have been taken to prevent such a break-in? If so, what sort of measures would be adequate to satisfy the requirements of due care?

3. Service Bureau Case

With regard to the standard of care required for a small service company, assume you are the attorney for the ABC Service Bureau, a small firm that performs outside data processing services for other companies. Assume that a new IRS regulation requires that employers who file a substantial amount of salary and pension information items on Forms W-2 or W-2P must do so using magnetic
As expected, several small and medium-size companies with insufficient data processing resources of their own contact ABC. While business prospects are good, ABC is concerned about its liability in the event of a break-in. Since tax information is highly sensitive, ABC wonders if it should accept the jobs; particularly if we assume terminal operators in offices throughout the state input data over telephone lines to the central office.

What if someone intercepted data in transmission, or somehow accessed the company's central files? What liability would ABC face if this personal tax and salary information were disclosed? What is the effect of a contract clause that ABC "use the utmost care at all times to protect the confidentiality of the data being converted"?²²

As ABC's attorney, you must determine the standard of care ABC will be held to in the event of a break-in. More practically, you must establish what ABC must do to protect itself from liability.

4. Additional Examples

Aside from liability in tort or contract, there are additional bases for liability caused by unauthorized access. For example, wrongful access or disclosure could result in violations of privacy, due process, or defamation. Several such possibilities, as suggested by recent literature, are listed briefly.²³

Although many diverse groups have legitimate needs for obtaining personal data, easy accessibility to this information raises privacy concerns. For example, hospital patient records may be accessed by insurance companies, government statisticians, and medi-

²¹ 26 C.F.R. § 301.6011-2 (1986). For tax year 1986, this regulation applies to employers who file 500 or more such forms. For tax year 1987, the threshold is reduced to 250 forms. If you don't comply, and haven't received a hardship waiver, you are deemed not to have filed, and may therefore incur all the attendant penalties.

The purpose of this regulation is to speed up tax processing of employee wage items. After 20 years of trying voluntary persuasion, the government finally gave up and concluded that it had no choice but to force businesses to modernize. IRS Requires Filing Tax Return Information on Magnetic Media, COMPUTER L. AND TAX REP., Sept. 1986, at 5.

²² See, e.g., R. RAYSMAN & P. BROWN, COMPUTER LAW: DRAFTING AND NEGOTIATING FORMS AND AGREEMENTS 10.05 [3]-[4] (1987). [hereinafter RAYSMAN & BROWN]. The vendor may be obliged to protect the client's data, but by what standards is that obligation measured? Is there a level of protection below which the vendor has breached the contract?

cal administrators. A patient's private life could be compromised by the disclosure of his medical file. An example would be an AIDS patient who loses his job because his medical condition was made public through unauthorized access to his computerized medical records. Additionally, law enforcement officials have proposed a national Computerized Criminal History (CCH) system as a means of gathering intelligence. Is it possible to maintain privacy or integrity in a database which contains information on tens of millions of persons and is accessible to tens of thousands of persons countrywide?24

In a less noble vein, databases have been developed listing over two million Americans who have filed malpractice and product liability lawsuits,25 and another listing over a half million women who wear petite dress sizes.26 The possibilities for additional personal data bases are endless.27 While each may be built up innocently enough, there are no standard procedures to protect against an invasion of privacy which might be caused by the unauthorized gathering and dissemination of the personal information generated. Due process concerns may also be raised by unauthorized computer access. For example, a computer network was designed in San Francisco which allowed individuals working from a local police department computer to access public defender files. While no due process violations were established, a court could have found a defendant's constitutional rights were infringed through a violation of the attorney-client privilege.28 So, even without evidence of actual wrongdoing, a potentially dangerous criminal could have been released through an inadvertent disclosure.29 Despite the magnitude of this mistake, there still appear to be no generally-accepted com-

24. See K. Landon, Dossier Society (1986). See also Olmos, Civil Rights Issues Fuel L.A.'s Warrant Systems Changes, COMPUTERWORLD, Oct. 29, 1984, at 10 (Incorrect computer data caused arrest of the wrong man. Time in jail forced him to drop out of college and be called to active duty for missing reserve meetings.) Error could have just as easily been caused maliciously by hackers as accidently.


29. Telephone conversation with Jay Bloom Becker, Director, National Center for Computer Crime Data (NCCCD), 2700 North Cahuenga Blvd., Los Angeles, CA 90068 (213-874-8233) (March 14, 1988) (advising that no actual violation had been found).
computer standards to prevent a recurrence of such an incident in the future.

Finally, unauthorized access may result in any number of claims against management. In the famous case of *Dun & Bradstreet v. Greenmoss Builders*, the company's management was held liable for defamation when a false and damaging credit report was produced due to the negligence of a poorly-supervised high school employee. The United States Supreme Court allowed punitive damages to be awarded without a showing of actual malice because the erroneous statements did not involve matters of public concern. A future case could just as easily find negligence and award punitive damages if the lack of computer security permitted hackers to corrupt the data base, causing defamatory statements to be issued.

These examples are not exhaustive. The potential for harm is as unlimited as are modern computer applications themselves. The question remains: are there applicable legal standards which indicate the minimum level of security needed to prevent liability from unauthorized computer access and abuse? E. General Standards of Care

1. Lack of Generally-Accepted Standards

Surprisingly, there are no generally-accepted industry-wide standards of due care for the protection of computerized data, and even more surprising is the fact that computer security principles have been well known to practitioners for over a decade. Thus, presently, enterprises which hold computerized data are virtually free from liability for harm caused by unauthorized access, even though methods to protect that data are common knowledge in the industry.

---

31. *Id.* at 763.
33. The first technical discussion of computer security in its own right was held in 1967. *Ware, Computer Security Standards for Government and Industry: Where Will they Come From?, Computer Security J.* 71 (Spring 1983) [hereinafter *Ware*]. Much subsequent research from that conference was classified until 1976. *Id.* However, computer security fundamentals filtered out to the business community starting in the early 1970's. *See, e.g.*, Martin, *supra* note 4; Hoffman, *supra* note 4. It is interesting to observe that the 1967 conference was held three years after the introduction of the modern "third generation" of computers, the IBM System/360, on April 7, 1964. G. SHELLY & T. CASHMAN, COMPUTER FUNDAMENTALS WITH APPLICATION SOFTWARE 2.12 (1986) [hereinafter SHELLY & CASHMAN].
2. Consequences of Lack of Standards

Although the lack of generally-accepted industry-wide (GAIW) standards of due care seem unbelievable to some, there are managers that feel the lack of standards is economical and even beneficial to their businesses. Without standards, they do not feel the need to purchase security software or encryption devices, develop and test contingency plans, or educate their staffs in security procedures. They believe that a victim’s attorney faces the insurmountable task of convincing a lay jury that a certain computer security technique is expected of persons with ordinary competence and standing in the business, that failure to implement this technique caused the damage, and that the business holding the data should be held liable for that damage.

Despite the shortsighted validity of these beliefs, the present lack of GAIW standards may harm these same businesses for two reasons. First, the lack of GAIW standards lulls businesses into a false sense of security that their failure to implement security systems cannot lead to liability. With the rapid advance of technology in modern society, liability for computer negligence seems inevitable, and businesses should recognize the risk of substantial liability in the future for their failure to implement security measures now. Juries, aided by expert witnesses, will eventually realize the injustice of a private enterprise shielding itself from liability solely by relying on the mystique of computers. Standards would provide some objective means by which a business could be reasonably certain that it has met its obligations to the public.34 Second, in addition to failing to protect individuals from unauthorized access, the lack of GAIW standards also fails to protect those same businesses from computer crime.35 Such standards would not eliminate computer abuse, especially by “insiders;” they would not eliminate computer-related negligence. They would, however, provide a “curb on technology,” a baseline from which to judge both compensation for victims of computer abuse and the efficacy of measures to combat computer crime.36

Many business managers believe that computer security con-

34. “A standard is something you put in place so that no one is penalized as you go to it in the future.” S. Diamond, Unscrambling Data Security, COMPUTERS IN BANKING, April 1987, at 76, 81.

35. Most computer security measures which protect individual privacy also, felicita-

tously, guard against computer crime. See generally MARTIN, supra note 4, Chapter 2;

FISHER, supra note 4, Chapter 5.

36. The fact that standards of due care for the protection of computerized data do not currently exist in the industry cannot, in itself, show that prudence does not dictate the need
controls are not cost effective to combat losses from computer crime.\textsuperscript{37} While there is an element of truth to this belief,\textsuperscript{38} standardized controls would bring about economies of scale that could ultimately lessen the financial burden.\textsuperscript{39} An understanding of the need for GAIW standards must start with an understanding of the principles of computer security.

### III. Computer Security Demystified: Identifying Problems of “Due Care” in the Protection of Computerized Data

#### A. The Need for Understanding

There are several reasons why a lawyer would need a working knowledge of computer security. First, she may be involved in tort litigation representing a plaintiff who has been injured by the failure of a business enterprise to protect its computerized data against hackers. Second, she may be involved in a criminal case where a critical question is the defendant’s right to access certain data.\textsuperscript{40}

---


\textsuperscript{38} As stated in the seminal text on computer security: “Security and accuracy controls increase the cost of a computer system and in some cases degrade its performance somewhat. Furthermore, they do not give absolute safety, but a measure of it.” \textit{J. Martin}, supra note 4, at 43. This is as true today as when written, but of course it is true in general of all administrative and regulatory systems, and the cost element is always less burdensome if the procedures are standardized.

\textsuperscript{39} Discussing encryption, which is absolutely essential for banks but not always utilized, one contemporary writer observed:

> Whether because of budget restraints or personnel shortages, encryption always seems to take second place to everything else on the priority list. . . . The situation may be changing somewhat since the banking committee of the American National Standards Institute (ANSI) is proposing standards related to encryption. A final encryption standard should be approved by early next year. Although the ANSI standards are not binding, they serve to increase awareness of security issues and act as rallying points for banks concerned about implementing security procedures.

Diamond, supra note 34, at 77 (emphasis added).


Some state statutes make the fact of unauthorized access itself an offense, without regard to actual harm caused (i.e., money theft, theft of services, invasion of privacy, malicious damage or disruption). \textit{Conn. Gen. Stat. Ann.} $\S$ 53a-251b (West 1985) reads in part:

1. A person is guilty of the computer crime of unauthorized access to a computer sys-
Third, she may be drafting a contract in which one party wishes to insist that the other use the utmost care in protecting computerized data, to the point of defining that level of care with technical specificity. Fourth, as counsel to firms dealing in computerized data, she may need a general understanding of that area to protect the firm from whatever problems might arise.

While lawyers think it obvious that one does not need to be a doctor to try a medical malpractice case or an architect to file suit for injuries sustained in a building collapse, it is just as obvious that one need not be an expert in computer internals to litigate or counsel on computer security matters. However, one must know some-

tem when, knowing that he is not authorized to do so, he accesses or causes to be accessed any computer system without authorization.

(2) It shall be an affirmative defense... that:

(A) The person reasonably believed that the owner of the computer system, or a person empowered to license access thereto, had authorized him to access;... or (C) the person reasonably could not have known that his access was unauthorized.

It is not always clear-cut whether a person “knew he was not authorized” to access a system, or if he “reasonably believed that he had been or would have been empowered to do so.” These factual questions may be influenced by the security that actually exists at the organization in question (i.e., how strong is password protection? How up-to-date are access rules? How seriously are violations handled? What security education and awareness efforts are undertaken, and at what level?) Further, it is unclear whether legitimate access to a system, followed by unauthorized access to certain data within the system, would be a violation. And what of access on Saturday, if an individual had been authorized access for weekday working hours only?

CAL. PENAL CODE § 502(d) (West Supp. 1987) reads in part: Any person who intentionally and without authorization accesses any computer system,.. or data, with knowledge that the access was not authorized, shall be guilty of a public offense. This... shall not apply to any person who accesses his or her employer's computer system,.. when acting within the scope of his or her employment. The reference to “or data” presumably handles the problem of legitimate access to a system followed by unauthorized access to certain data in the system. But the statute's exemption of employees acting within the scope of their employment invites the same types of questions as the Connecticut statute. “Scope of employment” will surely depend upon accepted organizational practices.

TEXAS PENAL CODE ANN. § 33.02 (Vernon Supp. 1989) reads in part: (a) A person commits an offense if the person:... (2) gains access to data stored or maintained by a computer without the effective consent of the owner or licensee of the data and the actor knows that there exists a computer security system intended to prevent him from gaining access to that data.

Of course, “effective consent” is another way of stating the problems raised by the Connecticut statute. The Texas statute appears to require that the business have a security system in place before initiating a prosecution. However, the degree of technical strength of the system, its level of maintenance, and its effective administration, are not defined. It is too easy to conceive of the existence of an ineffective "computer security system" whose sole purpose is to demonstrate an element of the offense!

41. Cf. supra note 22.
thing. This section attempts to guide the reader through a study of selected existing materials.\textsuperscript{42}

B. \textit{Functional Elements of a Computer System}

It is impossible to understand the language of computer security without a picture of the functional elements of a computer system. Figure 1 provides a simplified model of these elements. For a more detailed study, the reader is encouraged to purchase a copy of Shelly & Cashman.\textsuperscript{43} It is essential to understand the flow of information through the system, to appreciate the vulnerabilities and necessary safeguards for protecting computerized data in a cost-effective manner.\textsuperscript{44}

Input devices attached to the processor include keypunch, tape drives, key-to-disk systems, optical character readers, and magnetic ink character recognition units.\textsuperscript{45} Each device translates raw information into machine-readable data and places it into the computer processor's main memory; thus, these devices need to be physically attached to the processor.\textsuperscript{46}

\begin{itemize}
\item Many persons fear to delve into technical matters that may be "over their heads." But the truth is that no one is an expert on everything; the trick is to understand as much as you need so as to make proper use of experts when necessary. Even in the computer field, expertness is relative. Few of the top-flight computer programmers understand the engineering and physics necessary for digital computer hardware to function; very few understand the high-level algebra underlying compiler design, which permits them to write English-like code that a binary machine can operate upon. This presents no difficulty: they understand as much as they need to solve the problem at hand.
\item See \textit{Shelly \& Cashman}, supra note 33. The book is available from Boyd \& Fraser Publishing Co., Boston, MA. It is, in the author's opinion, the best introduction to computer fundamentals written to date.
\item The reader should understand that the model presented in this paper is not a textbook of computer fundamentals and cannot substitute for one. \textit{Shelly \& Cashman} is highly recommended for all readers not totally conversant with large-scale computer system theory. It is lavishly illustrated and superbly organized. One could profit from reading the entire text, including chapter summaries, but omitting research projects and software package instructions if time is limited. Even those persons fairly conversant with the subject matter could profit from the book as a reference and refresher for any uncertain concepts. This paper shall refer to it repeatedly in footnotes.
\item With regard to the model in Figure 1, see \textit{Shelly \& Cashman}, supra note 33, at 1.1-1.37 (reinforcement and illustration of model, including examples of large computer installations and personal computers for home and business use). \textit{See also id.} at 2.1-2.33 (evolution of computers from the early days to modern advanced applications).
\item Readers who instead desire a briefer, non-illustrated written summary of computer system fundamentals are referred to A. Beque, \textit{supra} note 4, at 94-103 ("Basics of the System," etc.).
\item See \textit{Shelly \& Cashman}, supra note 33, at 3.1-3.5.
\item See \textit{id.} at 5.1-5.33 (illustrated device descriptions).
\item See \textit{id.} at 4.1-4.27 (overview of input processing modes and brief introduction to data communications).
\end{itemize}
“Data communications” is the term commonly used for sending data over channels such as telephone lines, coaxial cables, microwaves, or fibre optics. A modem converts digital data from the communications terminal into analog signals suitable for transmission, then converts the analog signals back to digital data for computer processing. There are two methods for establishing the communication link between a terminal and processor: leased lines and switched lines. Leased lines are permanent connections be-

---

47. Data communications is also known as “telecommunications” or “teleprocessing.”
48. See id. at 11.1-11.13 (elements of data communications). Note that the network model shown as Figure 11.2 on page 11.3 fits our model.
between the two devices and are also known as "dedicated," "direct," or "private" lines. Examples include lines between the White House and the Kremlin or between a corporation's home office and its branch.

Since it is too expensive to have leased lines between devices throughout the country, switched lines, also known as "public" lines, are common. Switched lines are available from the telephone company and utilize standard telephone company switching devices. A data communications system in which users dial into the computer via switched lines has come to be known as a "dial-up system" and is particularly vulnerable to hackers attempting to enter the computer system.

The input data are read into main memory as application data. The application program, which tells the computer how to act upon this data, is also read into main memory, usually from auxiliary storage. In addition, portions of the operating system (O/S) are present in main memory. O/S is most easily thought of as "common routines," i.e., programs which may be used by all application programs, pre-written for data processing convenience.

The Central Processing Unit (CPU) is the "heart" of the computer and contains the circuitry which enables the system to function. The Control Unit handles the complex task of switching between various input/output devices and the processor in order to process data accurately and completely. The Arithmetic-Logic Unit (ALU) performs standard arithmetic operations and logical comparisons.

In theory, all the data needed to run the computer system could reside permanently in main memory or be entered via input devices. In practice, however, this is unworkable because of the


51. See SHELLY & CASHMAN, supra note 33, at 12.1-12.11 (general nature of application programs); see also id. at 13.1-13.13 (brief fundamentals of programming languages). For further information on the application development process, see id. at 15.1-15.15 (systems analysis) and 16.1-16.31 (program analysis).

52. See id. at 14.1-14.8 (brief overview of this incredibly complex subject). Note that O/S contains, in general, two types of programs: those which make it possible for the application program to function (i.e., load, compile, execute), and "utilities" which make application programming easier (i.e., sort and file management).

53. See id. at 8.14-8.17.

54. See id. at 3.5-3.9. A logical comparison determines if one data item is greater than, equal to, or less than another data item.
enormous volume of programs and data in typical organizations. Storing it all in the main memory would be too expensive and inputting it with each program run would be excruciatingly slow. Therefore, auxiliary storage typically holds the great majority of application programs, data files and tables used by these programs. Auxiliary storage is often referred to as an "electronic file cabinet." Devices include magnetic tape, hard disk, floppy disk or diskette, and certain exotic instruments such as bubble memory. Most software security systems are particularly concerned with protecting auxiliary storage since it is typically accessible to the full computer system and contains the master files for many different applications.

Output devices take data from main memory and record it physically. Typical output devices include printers, terminals, and plotters. However, certain output is not directly human-readable, such as computer output microfilm (COM) or voice output.

The model in Figure 1 remains accurate for any computer system as long as one important fact is recognized: a computer system is not limited to one set of input devices or one processor, nor must the input devices and processors all be located at the same site. Figure 2 illustrates a general "network", a logical grouping of computers and terminals connected by a communications system. Although a network has infinite possible configurations, they will all feature some kind of link among computers, terminals, and channels.

Each processor within a network will contain the components defined in Figure 1. However, instead of configuring the organization around one computer center as Figure 1 might imply, a computer system might be designed around organizational realities, often referred to as "distributed data processing." In addition to its universal application, Figure 1 holds for all known technologies. Computer system advances which increase speed, reliability, and flexibility, or which decrease cost, space, and power requirements, will not change any of the elements of the ba-

55. See id. at 9.1-9.19.
56. See id. at 3.9-3.10.
57. See id. at 6.1-6.27 (illustrated device descriptions). See also id. at 7.1-7.23 (illustration of actual user interface with computer system, using terminal as input/output device).
58. See H. KATZAN, AN INTRODUCTION TO DISTRIBUTED DATA PROCESSING 53, 119 (1978); SHELLY & CASHMAN, supra note 33, at 11.15-11.17 (illustration and amplification of this discussion).
59. KATZAN, supra note 58, at 53.
60. KATZAN, supra note 58, at 110.
sic functional model.61

C. Basic Elements of Computer Security

1. Note on Data Exposures

In order to develop a working knowledge of computer security, a lawyer needs to familiarize himself with its basic elements. However, the subject is too broad to be extensively covered in this article. Thus, this discussion will guide the reader through some selected existing material. For a deeper understanding of the concepts presented, the reader is encouraged to obtain copies of Husband and of Fisher.62

Computer security generally is concerned with the implementation of controls to meet exposures.63 Normally, however, only cost effective controls are considered.64 This implies that a business enterprise will measure the cost of a given security control against the reduced loss exposure which would result from its implementation and then decide whether and in what manner to install the control. Such a process is usually termed a “risk assessment” or “risk analysis.” The reader might assume that businesses regularly perform security risk assessments, but because of complications involved and the lack of reliability in the process, this is not the case.

61. This statement may be difficult for the layman to accept. The major reason for its validity is that basic computer architecture has not changed in principle since the “stored program concept” was developed by von Neumann in 1945. See Shelly & Cashman, supra note 33, at 2.4 (“although accepted as ‘modus operandi’ today, [the stored program] concept was a brilliant breakthrough in 1945.”); R.G. Garside, The Architecture of Digital Computers 1-31 (1980) (a magnificent text for persons conversant with basic computer internals).

62. See Computer Systems supra note 16; R. Fisher, supra note 4. Unfortunately, there is no one text, to the author’s knowledge, that does for computer security fundamentals what Shelly & Cashman does for general computer fundamentals. There are several excellent books and articles in the field, but as of this writing, there is no one single text which is consistently at the proper level for lawyers: some are too technical, some are too wordy, some are too product-specific, etc. Most of what is needed can be found in these two books, and this paper shall refer to them frequently in footnotes.

COMPUTER SYSTEMS, supra note 16, also contains valuable information on software piracy, protection of proprietary rights, and state and federal computer crime legislation. The author highly recommends this text for computer lawyers with a technical bent.

It should be noted for completeness that the seminal text in computer security is J. Martin, supra note 4. All computer security books owe a debt to Martin and usually acknowledge that. The best readable technical book in the field is L. Hoffman, supra note 4. This paper shall occasionally refer to it in footnotes, but it is optional for the general reader.

The author apologizes for any injustice done to other authorities. New materials continually appear in this field, but we have to start somewhere.

63. See supra note 4.

64. See Computer Systems supra note 16, at 179; R. Fisher, supra note 4, at 80.

65. “Typically, a risk assessment process is used to select a combination of management
It is virtually impossible with current technology to determine precisely the total set of exposures, the potential annualized loss from each exposure, the true cost of often-overlapping controls, and the resulting reduced annualized loss from each exposure. Therefore, in practice, controls are generally implemented only after an exposure occurs and is recognized as a problem by management.

There is no known general model of computer security exposures. Therefore, even though the very definition of computer security implies that the lawyer must study data exposures in as much detail as data controls, in practice, this is impossible. A lawyer may safely assume that huge potential losses may result from the accidental or intentional disclosure of data to unauthorized persons, or from the unauthorized modification or destruction of data. In view of the enormous potential for loss caused by data exposures, it is clear that controls are essential to protect individuals and businesses.

and technical controls that provides protection from those risks which are of most concern."

COMPUTER SYSTEMS supra note 16, at 180.

"[T]he most appropriate time for a [risk analysis] is before the consideration of controls." R. FISHER supra note 4, at 81 (emphasis in original).

These statements, while perfectly logical, amount to "wishful thinking" in today's computer security environment.

66. See R. FISHER, supra note 4, at 82-98, for a description of the standard risk assessment process. The extreme complications necessary to achieve a result in which no one has much confidence explains why the method is generally in disuse. No doubt one day, as controls are standardized and as consequential losses due to security exposures are better understood, there will exist more satisfactory risk assessment algorithms.

67. See R. FISHER, supra note 4, at 51-53, for a good brief general outline of data security exposures. With regard to the Figure 1 model, certain general examples of data exposures are apparent. This is by no means an exhaustive list:

(1) Input devices: passwords and general instructions taped onto terminals; looking over someone's shoulder to "steal" a password; dialing in to a computer system not authorized for your use; entering fraudulent data.

(2) Communication Channels: wiretapping; sabotaging lines.

(3) Processor/Computer Center: fire, flood, and other Acts of God; riots and sabotage; power failure and brownout.

(4) Application Programs: logic bombs (computer virus or other software sabotage); program errors; erroneous duplicate processing.

(5) O/S: unauthorized access to O/S, which disrupts all application programs.

(6) Auxiliary Storage: unauthorized access to another's files (intentional or not); dropping tapes and disks; writing over live data on media.

(7) Output: routing sensitive output to the wrong terminal; using proprietary printouts for scrap paper; stealing or selling output.

68. See supra text accompanying notes 23-31 for some practical examples. No one quite knows the cost of computer crime in the U.S. One oft-quoted figure is that white collar crime losses exceed $40 billion annually in the private sector alone. A. BEQUAI, supra note 4, at 6. Computer-related crime must comprise a portion of this figure.

69. The reader is reminded that the following discussion of computer security controls is not a textbook and cannot substitute for one. It is intended, along with the previous sec-
2. Categories of Controls

There are an infinite number of security measures which can be taken to protect against accidental or intentional exposures. However, to simplify this discussion, this article considers computer security controls as a system of five major categories.70

a. Physical Security Controls

Physical security controls have two main objectives: to restrict access to facilities, and to protect hardware and software from damage, to give the lawyer a working knowledge of the general nature of computer security. The appropriate textbook in the area has yet to be written and probably will not be until a greater degree of standardization develops.

70. Every writer expresses it a little differently, but the categories presented here are not inconsistent with those of any recognized authority.
age if disaster occurs. These are the "traditional" controls which previously consisted of locks, guards, and fences. Today they may encompass such sophisticated devices as minicomputer-driven access restriction mechanisms, smoke detection devices and concealed alarm systems.

Although physical security controls are essential to a properly-secured environment, they are inadequate by themselves for two reasons. First, many offenses against data are committed by fully authorized persons. Second, with modern data communications technology, it is no longer necessary to be physically located at the data center to cause harm to the system.

b. Access Control Software

Access control software consists of mechanisms built into the computer system itself with three objectives in mind: to keep unauthorized users out of the system, to restrict authorized users to data specifically allowed to them, and to report attempted violations for corrective action. Access control software is the heart of any computer security system. Its viability clearly depends upon proving the identity of the person attempting to access the system. This is usually done via a password.

Although access control software is essential in any modern computer security system, it is inadequate by itself. It does not solve the problem of wiretapping communication lines, and as a technical measure, it offers no self-assurance that it is being correctly implemented and controlled.

c. Dial-up Controls

Recall that data communications users may access a system using one of two communication methods: leased lines or switched (dial-up) lines. If secure access control software is in place, then

72. See R. Fisher, supra note 4, at 147-49 (questionnaire which illustrates the general range of physical security controls). The reader may recall that organizations once were proud to "show off" their data centers to the general public; very few do so now, as that is considered a "security risk."
73. See supra notes 42-49 and accompanying text. 74. See Computer Systems supra note 16, at 187. With regard to the Figure 1 model, these controls are intended to: prevent unauthorized users from accessing the system via terminals; prevent authorized users from accessing data in main memory or auxiliary storage except as specifically authorized for them and in the manner authorized; and produce output sufficient to permit system administrators to take prompt and responsible action against violators. These controls are considered in more detail in § III-D infra.
75. See supra note 49 and accompanying text.
the communication method should be totally irrelevant as far as security is concerned. Hackers with the installation phone number will still be prevented from accessing the system by lack of a valid password. However, as subsequently discussed, access control software is far from ideal, and the weaknesses of passwords as an authentication device is legendary. Therefore, since hackers will often try to access a system via dial-up, many installations use dial-up security controls to provide an additional level of security.

Dial-up security devices are often known as port protection devices (PPDs). Presently, PPDs use one of two general methods to increase security over traditional access control passwords.

The first method requires all dial-up users to enter an “access code,” often via touch-tone pad on their telephone set or via the terminal keyboard itself. Once this code is accepted, the user is in the system, but he will still be subject to any access control software measures that exist. In effect, the access code is an additional password; thus, the hacker must know two passwords instead of one in order to gain access to the computerized data.

The second method features what is known as “call-back.” The system associates a telephone number with each user’s access code. Upon receiving a valid access code, the system disconnects the caller and automatically places a return phone call to the expected number. If that call goes through, connection to the system is established. Therefore, the hacker must not only have a valid user’s access code but must be at the valid user’s expected location as well. Call-back provides an extra measure of security, but it is not extensively used as of this writing. Drawbacks include: extra time to make the connection, extra phone costs, and lack of flexibility for dealing with legitimate mobile users such as traveling salespersons. PPDs do, however, fill the void left by access control software. Thus, despite their inconvenience, their use may be justified where system data is extremely sensitive and additional protection is needed.

---

76. See infra notes 121-35 and accompanying text.
77. See COMPUTER SYSTEMS, supra note 16, at 186.
78. See id. at 199-200.
79. Id. at 200-201.
80. PPDs raise additional questions of their own, such as: how many tries should be allowed to enter the correct access code? Should PPD’s be managed by a group different from that managing access control software? Id. at 201-202; see also id. at 202-207 (more advanced discussion of technological considerations for device selection).
81. The author is aware that PPD’s have occasionally been used in installations that have no meaningful access control software. In that case, they are not an additional level of security, but rather the only level. The best one can say for this situation is that it is better
d. Encryption

Despite the system protection provided by access control software and PPDs, the communication channel itself is still unprotected. Encryption, concealing information by rendering it unrecognizable to persons who do not possess decryption devices, is the only known defense to wiretapping. In general, an "encryption key" is used to encode data, and the same key must be used to decode the data.

There are two main types of encryption line encryption is the traditional type and protects data sent over communication channels and file encryption protects data while it resides on auxiliary storage. Intruders who managed to access a file without authorization or managed to physically steal the device from the computer center would still find that file unreadable unless they also had the encryption key.

Specific cryptographic devices are now being developed to handle new types of equipment and communication technology. They vary widely by factors such as the extent of data protection within the computer system, ease of use, strength of the encryption algorithm, and implementation method.

e. Administrative Controls

Despite all of the protection provided by the technical controls discussed above, access control software, PPDs, and encryption, coupled with physical security, the security system may still be inadequate to protect an organization. Proper installation does not ensure proper control and coordination of the devices, user education, or preventive future planning.

---

82. See id. at 187; see also L. HOFFMAN, supra note 4, at 42-91 (more technical discussion of general cryptographic methods and their implementation in hardware and software).
83. See COMPUTER SYSTEMS supra note 16, at 215.
84. See id. at 207, 214.
85. See id. at 214-215 (“Communication Protection”).
86. See id. at 215 (“Storage Protection”); see also supra note 55 and accompanying text (discussion of auxiliary storage devices).
88. “The object of security education must be to obtain security by consent. It should never be imposed without reason. Security must be seen to be reasonable and necessary. . . .” J. MARTIN, supra note 4, at 393.
89. The author, along with most other computer security professionals, has dozens of "war stories" discussing fine technological devices which were rendered useless due to poor implementation and administration. In general, technical controls are implemented by technicians, who view computer security as a technical problem, and one which hopefully will not
Administrative security controls establish and maintain policies, procedures, and guidelines to ensure that computer security mechanisms are properly utilized. Administrative controls include such measures as the establishment of a separate security unit within the organization; promulgation of security awareness and education; personnel policies such as job rotation, separation of duties, and background checks; contingency planning; miscellaneous devices such as business interruption insurance, inventory control, and proprietary labelling; and, most recently, protection against computer viruses.

Ideally, administrative controls should be developed simultaneously with sound technical controls. Weak administration can cause improper coordination with the technical controls, and weak technical controls can reduce administrative controls to mere window-dressing.

D. Access Control Software Models

Access Control Software (ACS) as a security device must now be considered in more detail. Assume that the ACS File is a file of operating system data, “common routines” which reside in the main memory. The ACS file performs several specific functions which will be considered below as a system of five categories.

1. Identification

ACS requires that all users be identified and held accountable for their actions. Identification requires that a unique code, called inhibit them in their special work. While computer security cannot function in a modern environment without sophisticated technology, clearly it must be administered by persons who sympathize with its overall purpose of ensuring that individuals and businesses are adequately protected.

90. Responsibility for computer security should not be delegated to persons who are evaluated on the basis of computer system performance. Such delegation is analogous to assigning bank tellers to audit the daily cash flow.


93. See id. at 152-53 (“Application Development” questions).

94. See McAfee, The Virus Cure, Datamation, Feb. 15, 1989, at 29. A computer virus is essentially the corruption of application programs or O/S routines, often by a perfectly legitimate user. Software to prevent, detect, and recover from computer viruses has begun to be developed. Anti-viral devices are in their infancy at this writing, but will surely come into their own in the near future.

95. See supra text accompanying notes 50-52.

96. Again, the terminology is not standardized, and authorities list anywhere from three to six major functions of access control software. The categories and models represented herein are generally consistent with the writings of any recognized authority.
an ID-Code\textsuperscript{97}, be established for each system user on the ACS file. When a user attempts to access the system, the ACS file is checked for the ID-code. If the ID-code is not present, access is denied.\textsuperscript{98}

![Fig. 3](image)

\begin{tabular}{|l|l|}
\hline
ID-CODE & MISC-DATA \\
\hline
USER-1 & \_\_\_ \\
\hline
USER-2 & \_\_\_ \\
\hline
USER-3 & \_\_\_ \\
\hline
\end{tabular}

Surprisingly, ID-Codes are non-secret. The ID-Code is typically printed in numerous documents and reports that traverse the organization. Unique identification is necessary for ACS file rules to be meaningful and unambiguous.\textsuperscript{99}

2. Authentication

Identification is merely a claim of identity. Anyone can sit at a terminal and type an ID-code, especially when these codes are non-secret. Authentication is the means of validating the person entering the ID-code.

The most common authentication device is the password. Suppose that a password is recorded for each user on the ACS file. After the user enters the ID-Code and is verified, the user must then enter his password. If the password is not matched to the password in the ACS file, access is denied.\textsuperscript{100}

\textsuperscript{97} Also variously known as a Logon-ID, Account Number, or User-ID.

\textsuperscript{98} See Figure 3. This illustrates three users (ID-Codes) on the ACS File, identified as USER-1, USER-2, and USER-3. Certain miscellaneous data is normally associated with each ID-Code, such as: Name, Department, Unit, Title, phone number, etc. If a person entered "USER-4" as an ID-Code at the terminal, that person would be denied access to the system.

\textsuperscript{99} See also R. Fisher, supra note 4, at 25.

\textsuperscript{100} See Figure 4. A password is associated with each ID-Code. The user will not be allowed to enter the system unless the password he enters at the terminal matches the password on the ACS file. In this case, USER-1 must enter password "LAWYER," or be denied access to the system.
Passwords as an authentication device have two major weaknesses. First, it is fairly easy to crack most passwords mathematically.\textsuperscript{101} Second, the tendency of persons to choose easily-remembered (and thus easily-guessed) passwords, or even to write these passwords down in an obvious place, is part of security folklore.\textsuperscript{102} Thus, security personnel have long been seeking stronger authentication methods.\textsuperscript{103}

Generally, there are three authentication methods for a user: something he knows (i.e., password); something he has (i.e., magnetic card); something he is (i.e., finger length, retinal pattern, signature characteristics). If one of the latter two methods is used, the authenticating data would be digitized and placed in a password field on the ACS file. The user’s possessed item or personal characteristic would be compared to this field.\textsuperscript{104} Non-password authentication has not received general acceptance, largely due to cost and reliability factors.\textsuperscript{105}

\begin{table}[h]
\centering
\begin{tabular}{|c|c|c|}
\hline
ID-CODE & MISC-DATA & PASSWORD \\
\hline
USER-1 & - - - - & LAWYER \\
\hline
USER-2 & - - - - & CLIENT \\
\hline
USER-3 & - - - - & JUDGE \\
\hline
\end{tabular}
\caption{ACS FILE: AUTHENTICATION}
\end{table}

\textsuperscript{101. See L. Hoffman, supra note 4, at 9-11 for technical details. For example, a 3-position password, alpha/numeric, has \((36)^3\) or 46,656 possible combinations; not an insurmountable number for attack by computer.}

\textsuperscript{102. A favorite anecdote among security professionals is that of the expert who, given someone’s personnel file, could guess his or her password within 10 tries in 90% of the cases. The author’s personal experience supports this story, at least for systems which have no restrictions on the passwords a user may choose.}

\textsuperscript{103. Password secrecy is sometimes enforced by encrypting the password on the file. Even if the full ACS File is not encrypted, as normally it is not, the password field in each user record should be.}

\textsuperscript{104. See R. Fisher, supra note 4, at 26.}

\textsuperscript{105. In the author’s opinion, non-password authentication is surely coming. Note that there are variations on simple passwords, such as requiring the user to answer a series of predetermined questions (mother’s maiden name, etc.) This has never caught on as it is too}
3. Authorization

Assuming that a user has accessed the system via ID and password (or other authentication device), it does not follow that the user should be able to access every file available to the system. Authorization states what resources a valid user may access and in what manner he may access them. Any attempt to access unauthorized files will be denied.

Fig. 5

ACS FILE: AUTHORIZATION (ELEMENTARY)

<table>
<thead>
<tr>
<th>ID-CODE</th>
<th>MISC-DATA</th>
<th>PASSWORD</th>
<th>FILES</th>
</tr>
</thead>
<tbody>
<tr>
<td>USER-1</td>
<td>- - - -</td>
<td>LAWYER</td>
<td>FILE-A</td>
</tr>
<tr>
<td>USER-2</td>
<td>- - - -</td>
<td>CLIENT</td>
<td>FILE-B</td>
</tr>
<tr>
<td>USER-3</td>
<td>- - - -</td>
<td>JUDGE</td>
<td>FILE-A FILE-B</td>
</tr>
</tbody>
</table>

Authorization may put conditions on system access. For example, a given user might be able to access a given file, but only from a certain terminal or terminals, at certain times of the day or on certain days of the week; or to read but not update. Furthermore, conditions may be combined, i.e., a user may read the Payroll file from any terminal, but update only those persons with salaries under $30,000.00, and only on weekdays from terminals located in the home office.

In general, any system element that a user might access is, theoretically, a resource whose access can be restricted based on conditions.

106. Recall the definition of access, see supra note 3.
107. It would be just as foolish to state that an employee who belongs in an office has an automatic right to look through every file cabinet and desk drawer in that office.
108. See Figure 5 for an example. If USER-1, a valid user who signs on with the proper password LAWYER, tries to access FILE-B, that access would be denied.
109. That is, User JONES might be restricted to signing on from Terminal 15, or be allowed to sign on from any other than Terminals 20 or 29. This is different from saying that he may access the Billing File provided he is on Terminal 15 only. The former is a "sign-on" (ID/Authentication-type) restriction; the latter is a file resource (authorization) restriction.
This may include restrictions on things like application programs or programming languages.

Fig. 6

ACS FILE: AUTHORIZATION (INTERMEDIATE)

<table>
<thead>
<tr>
<th>ID-CODE</th>
<th>MISC-DATA</th>
<th>PASSWORD</th>
<th>FILES</th>
<th>CONDITIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>USER-4</td>
<td>-----</td>
<td>MOTION</td>
<td>FILE-M</td>
<td>NONE</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>FILE-R</td>
<td>1. READ</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2. UPDATE ONLY FOR DATA ITEM UNDER $100,000.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>FILE-V</td>
<td>1. READ FROM HOME OFFICE TERMINAL ONLY</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2. UPDATE FROM TERMINALS 12 &amp; 14 ONLY, BETWEEN 9 - 5 LOCAL TIME ON WEEKDAYS.</td>
</tr>
</tbody>
</table>

In practice, authorization is conceptually more complex than it would seem. At its advanced level, instead of directly stating resources and conditions for each user, tables are established for each resource stating who may access the resource and in what manner. Further, instead of actually naming the users allowed by ID-code, the table may list groups of users, and the individual in question must be a member of the proper group. Conceptually, this has the same effect as the authorization rules discussed, but the advanced methods permit the greater flexibility needed for large organizations.111

110. See Figure 6 for an example. If USER-4 signed on to the system with a valid ID-Code and password, then tried to read FILE-V from a terminal located in a branch office, access to FILE-V would be denied.

There are no specific limits on conditions that may be imposed on file access. The ones mentioned in the text, however, illustrate types of restrictive conditions that one would expect to find in use today. See also L. Hoffman, supra note 4, at 23-27 (additional technical explanation).

111. See Figure 7 for an example. Each user must be added with a GROUP CODE to permit resource access decisions to be made. For example, User-A (Group Code G-1) could access File-M, but for read only, not update. If User-A, a valid system user, tried to access File-M for update, or tried to access File-X for any purpose, access would be denied.

This method seems quite a bit more tedious than the former ones. However, in a modern large computer network, with thousands of resources and tens of thousands of users,
I. FILES

<table>
<thead>
<tr>
<th>FILES</th>
<th>GROUP ACCESS</th>
<th>CONDITIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>FILE-M</td>
<td>G-1</td>
<td>READ ONLY</td>
</tr>
<tr>
<td></td>
<td>G-2</td>
<td>UPDATE IF UNDER $50,000</td>
</tr>
<tr>
<td>FILE-X</td>
<td>G-2</td>
<td>NO RESTRICTIONS</td>
</tr>
<tr>
<td></td>
<td>G-3</td>
<td>READ ON WEEK-DAYS ONLY</td>
</tr>
</tbody>
</table>

II. USERS

<table>
<thead>
<tr>
<th>ID-CODE</th>
<th>MISC-DATA</th>
<th>PASSWORD</th>
<th>GROUP CODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>USER-A</td>
<td>-----</td>
<td>-----</td>
<td>G-1</td>
</tr>
<tr>
<td>USER-W</td>
<td>-----</td>
<td>-----</td>
<td>G-2</td>
</tr>
<tr>
<td>USER-Y</td>
<td>-----</td>
<td>-----</td>
<td>G-2</td>
</tr>
<tr>
<td>USER-Z</td>
<td>-----</td>
<td>-----</td>
<td>G-3</td>
</tr>
</tbody>
</table>

In summary, authorization restricts the files a valid user may bring up once he has legally accessed the system. It can be relatively straightforward or quite sophisticated, stating very detailed access conditions. Authorization is without doubt the most important element of technical computer security.112

112. For the sake of completeness, authorization must be distinguished from file passwords. Before modern access control software, it was common to specify that certain key files, such as the Payroll File, could not be accessed unless the user supplied a "file password." This could be enforced by software, and administrators were responsible for disseminating the password to the proper persons (ideally changing it on occasion).

File passwords, of course, provide no basis for user accountability, as one cannot tell who has actually accessed the file. Today they are best used as an additional security device.

---

there is no practical alternative. If done correctly, this method has the same effect as that of Figure 6. See also R. FISHER supra note 4, at 26-28.

112. For the sake of completeness, authorization must be distinguished from file passwords. Before modern access control software, it was common to specify that certain key files, such as the Payroll File, could not be accessed unless the user supplied a "file password." This could be enforced by software, and administrators were responsible for disseminating the password to the proper persons (ideally changing it on occasion).

File passwords, of course, provide no basis for user accountability, as one cannot tell who has actually accessed the file. Today they are best used as an additional security device.
4. Logging

Even assuming that the authentication and authorization functions are working perfectly, there is nothing thus far to stop an intruder from signing on with a valid ID-code and trying every possible password until he stumbles across the correct one. Should that happen and the organization suffer a serious loss, management would surely wish that it had kept a record of actions against the ACS file so that it might be able to discern what happened, plug the leaks, and possibly recover from the violation. This is exactly the function of logging (also variously called journalling or recording).

Logging is the electronic recording of significant ACS file activity. Such activity will normally include all access requests which the security system denied such as invalid password attempts, or any valid requests which the system administrators somehow deemed worthy of inclusion. The purposes of logging are to catch actual malefactors, deter potential malefactors, and provide information for system recovery.

5. Monitoring and Surveillance

Logging normally results in the production of violation reports, or hard-copy listings of potential security violations. Management should monitor these reports and take appropriate action to identify and correct problems as early as possible.

Such external actions, however, are not the exclusive method of surveillance. Suppose that one specific ID-Code requests, say, five file accesses in one terminal session, all of which are denied. The ACS software might automatically “suspend” the ID, meaning that it can no longer sign on to the system until a system administrator investigates and “unsuspends” the ID.

In very advanced systems, a security console might be notified for very sensitive files, just as PPD's are used as an additional security device for dial-up users. See supra text accompanying notes 75-81.

113. Many good systems do not record invalid password attempts, since the huge majority of those are simple keying errors. However, logging may record the fact that one ID-Code had breached some threshold, such as ten password errors, in a single terminal session.

114. See FISHER, supra note 4, at 29. It is also common to use logging as an electronic record of all changes to the ACS File itself. Id. at 36.

115. The author has actually seen access control systems, with identification, authentication, and authorization, that offered no system logging of any kind. Apparently the management felt that logging was and monitoring were not worth the cost.

116. In terms of the model, Figure 4, assume that MISC-DATA contains an item called SUSPEND. If it is “on,” then the user cannot access the system, even if entering the correct password. This method is administratively preferable to deleting the entire user record, then having to re-enter all of it later.
of attempted violations in progress, and a security administrator
could call an officer to the terminal.\textsuperscript{117} It is also possible to keep a
real-time "trace" on users or terminals suspected of illicit activity.
This is the electronic equivalent of a police "stake-out".

E. Selected Problems in Computer Security Implementation

There are several commercially-available software packages
which purport to implement the computer security controls dis-
cussed. The layman might assume that since the basic principles of
computer security have been well known to practitioners for over a
decade\textsuperscript{118}, all that is needed to solve the problem of unauthorized
access is to install one of these security packages and assign a staff
person to be in charge of it.

However, in order to appreciate the concept of due care with
regard to unauthorized access, it is necessary to have a deeper un-
derstanding of some of the day-to-day problems in computer secur-
ity. The following examples demonstrate that the mere
implementation of basic computer security controls may be insuffi-
cient to protect against information abuse; more "curbs on technol-
ogy" are needed.\textsuperscript{119}

In an area as dynamic as this one, it is impractical to perform
an exhaustive survey of all computer security problem situations.
However, the lawyer who studies Part III should acquire at least a
working vocabulary of computer security and thus be able to deal
with the experts in the particular situation under consideration.\textsuperscript{120}

1. Proving Identity

As discussed previously, the usefulness of access control
software depends in part upon its ability to validate the identity of
the person attempting to access the system\textsuperscript{121}, and the device most
commonly used in validation is the password.\textsuperscript{122}

Suppose that an organization has implemented access control

\textsuperscript{117} See R. Fisher, supra note 4, at 29-30. Such "real time" surveillance represents the
state-of-the-art in logging functions. More commonly, a terminal will be "locked" after some
number of violations have emanated from it, and the user must initiate a call to the security
administrator to have it "unlocked."

\textsuperscript{118} See supra note 33 and accompanying text.

\textsuperscript{119} Cf. supra note 2.

\textsuperscript{120} Much knowledge in the area of computer security exists informally among practi-
tioners, sometimes printed in working papers or brought up at conferences, sometimes pub-
lished in specialized journals, sometimes just whispered. Unfortunately, no definitive text yet
exists.

\textsuperscript{121} See supra § III-D-1.

\textsuperscript{122} See supra § III-D-2.
software, but an intruder nevertheless gains access to the computer system by using another person’s password. Can it be said that the organization has done all that was reasonable to ensure protection of its computerized data against unauthorized access and should not be held liable for injury to an individual?

The plaintiff may argue that the defendant company failed to follow any of several “known” password protection practices. Specifically, defendant should have: mailed the password to the actual user in a “Personal and Confidential” envelope; required confirmation of receipt of the password\textsuperscript{123}; required the user to change his password at least once every 90 days\textsuperscript{124}; not permitted the password to contain vowels or duplicate characters\textsuperscript{125}; monitored the area to ensure that passwords were not posted on walls, terminals, or placed conspicuously in desk-top in-trays; conducted education programs to persuade users not to choose “trivial” passwords\textsuperscript{126}; not allowed a changed password to be the same as one of the last three

\begin{itemize}
\item [\textsuperscript{123}] These two situations apply when the user’s initial password is centrally-selected, but not of course when the user himself selects the password.
\item [\textsuperscript{124}] A common saying among practitioners is that “A password which is never changed is but an extension of the (non-secret) ID.”
\item [\textsuperscript{125}] It is well known among practitioners that limiting the use of vowels and requiring some numbers in the password will lessen the chance of its being guessed. Of course, it may also lessen the chance of its being remembered by the user and may thus cause him to write it down. Regarding the precise formula, practitioners generally feel that there should be limits on allowable passwords.
\end{itemize}

Some software security systems permit installations to enforce restrictions on password selection \textit{if they so choose}. Sometimes the attempt to enforce restrictions is relaxed to the point of absurdity:

“UNIX [a popular operating system known for its user-friendliness] requires, at least in one version, that a password should be a string of at least six characters, with the additional requirement that [it] contain at least one numeric and one non-alphanumeric [i.e., special character such as asterisk.] This is a reasonable requirement and UNIX imposes it, not once but twice. . .But on the third attempt to introduce [a non-complying] password or, indeed, any password, UNIX will accept it. . .[I]t is not difficult to imagine how many passwords, in practice, comply with the rule of having at least six characters including two odd ones.” I.S. Herschberg, The Hackers’ Comfort, Computers & Security, April 1987, at 133, 134.

Even if this particular loophole is closed, there is nothing to prevent future loopholes from arising in the name of “user-friendliness.”

\begin{itemize}
\item [\textsuperscript{126}] In some 40\% of the cases [surveyed], Mr. Baker’s password was also BAKER and similarly for Messrs. Smith, Jones, and so on. This in itself is no news; it merely confirms what has been found on many, too many, previous occasions . . .[T]he user . . .is loath to exercise his imagination to the extent that he not only serves his own comfort . . .but thereby greatly contributes to the hacker’s comfort.
\end{itemize}

\textit{Id.}

The author’s own experience as a data security administrator supports the belief that users will frequently choose trivial passwords.
passwords that the user had chosen; logged password violations, or if already logged, investigated repeated attempted violations; allowed the user to change his password on demand if he suspected a compromise; encrypted the passwords themselves on the access control file; used password suppression on terminals; displayed a "Last Sign-on Message" at the terminal; periodically verified that users still worked with the company and were thus entitled to retain their ID and password.

The defendant company will undoubtedly produce its own experts to testify that while each of the above is favored by some practitioners and may have been discussed at security conferences and work sessions, their use is an internal company matter subject to the normal business decision-making process. These devices are hardly "standards" by which liability to an individual may be judged.

This is all quite true. No standards currently exist to specify precisely what "password authentication" means. However, imagine a bank purchased a cheap vault with a shoddy lock capable of being opened with toothpicks; the mere fact that the bank had a vault may be insufficient to avoid liability. Yet, the mere fact that a company has some method of computer security may shield it from liability despite the ineffectiveness of the security system itself. Suffice it to say that the fact that an organization has access control software with passwords is no guarantee whatsoever that unauthorized persons cannot access the system.

The industry has long been aware that password authentica-

127. Users have been known to rotate trivial passwords, i.e., select AAAA, change it to BBBB, then back to AAAA, ad infinitum.

128. Normally certain technical programmers can read the access control file. Encrypting the password provides another measure of security for the password against these experts.

129. It is good practice, but not universal, for a password typed at a terminal to not be displayed. This causes problems for poor typists but is the rule today in most installations.

130. When a user signs on to a terminal, this message tells him when he last signed on. If he knows that he did not sign on at that time, then he can report a possible compromise to system security administrators.

131. Surprisingly few organizations will tie the Personnel System into the Security System. A person may leave the company, give his ID and password to a friend, and the ID is never deleted from the system. No one knows who "really owns" each active ID.

132. Even if all the above objections are met, consider this question: if a user signs on to a terminal with a valid ID and password, and subsequently, before signing off, there is a period of inactivity at the terminal, should the system automatically log the user off the terminal? The problem, of course, is that the user might have been called away on what he thought was a brief distraction and ended up away from the terminal permanently, forgetting that he was signed on. Should there be so-called "Idle Time" restrictions, whereby the user must re-enter his password or be denied access? If so, how many minutes of idleness qualify, and should that be a mandatory standard?
tion is inadequate. However, alternatives require extremely expensive pieces of specialized equipment which are not cost effective for individual organizations. Thus, the development of alternative authentication devices is left to vendors and their perception of market demand. To date, however, vendors are not persuaded that it is worth their while to develop alternatives. Thus, as long as there are no standards for imposing liability for computer abuse, businesses will not spend money to achieve a higher level of security, and there will be no incentive to vendors to develop more sophisticated computer security tools.

In addition to the inability of current authentication methods to prevent unauthorized access, these methods also offer little help in fighting computer crime. Suppose that a legitimate employee embezzles funds by attacking computer files. Police trace his identity through the system logs which show activity based on his ID-code as authenticated by his password. The prosecutor may think that he has an identification method as strong as a fingerprint, but any defense attorney should be able to prove the inadequacy of a password as the basis for a felony conviction.

In summary, access control software might serve to protect computerized data against unauthorized access if the identity of the person attempting to access the system can be proven. However, the current level of computer authentication offers no guarantee that such identity can be ascertained with any reasonable degree of certainty. If there are no standards for authentication to which business must adhere, then victims may go uncompensated and criminals unpunished.

133. "Current [user authentication] technology allows for voice, signature and other forms of identity verification. Based on widespread use and the absence of a generally acceptable alternative, the password facility is expected to continue. A cost effective alternative to passwords should be developed." W. Zopfi, J. Ludwig, E. Dominy, A. Hasegawa, Future Directions for an Information Security Architecture (July 13, 1986) (unpublished manuscript) at 7 [hereinafter cited as Directions]. Directions was presented at GUIDE 65, an IBM users' group, meeting in Chicago, July 13-18, 1986. Its purpose was to discuss security requirements in IBM products, with a view towards pressuring IBM as well as other vendors into offering meaningful security controls. Id. at Foreward.

134. "We believe signature authentication to be the most secure technology available today but we have not succeeded in finding sufficient applications to justify the development of a product." L. Wills, Security Strategy Response (March 18, 1987) (unpublished manuscript) at 8 [hereinafter cited as Response]. Response was presented at GUIDE 67, meeting in Anaheim, Cal., March 16-20, 1987. Its purpose was to serve as IBM's answer to Directions, supra note 133. Response at 2.

135. Cf. supra note 35.
2. Restricting File Access

Suppose that an organization has implemented access control software and a valid user injures another individual by accessing restricted data\(^{136}\), using his own ID-code and password. Can it be said that the organization did all that it reasonably could to prevent unauthorized access to restricted files? Should that organization be held liable for injury sustained as a result? This question is considered in detail by examining three situations.

\textit{a. Sensitive Residue}

When a user at a terminal requests a file, the data appears to be transferred directly from storage to the terminal screen. When the user finishes, the data appears to return to storage. Theoretically, the data is protected, since a user should be able to retrieve from auxiliary storage only those files permitted to him.

However, this is not actually the case. When an authorized user requests a computer file, the data is not directly transferred to the terminal screen. Rather, the data first goes to the computer’s main memory.\(^{137}\) The data stays in main memory, \textit{even if the user writes the file back into storage}, unless specific action is taken to clear it.\(^{138}\) While it is theoretically possible for the computer system to clear the data in memory automatically, this is cumbersome for a number of technical reasons; and, in practice, it is nearly always necessary for the user to clear the data.\(^{139}\) The risk is that if data is not cleared from memory, it can be read subsequently without undertaking unlawful access.

Some books and articles on computer security mention this problem; some do not. Is it standard knowledge among practitioners? Would management be negligent for failing to insist that users clear memory and for failing to audit such compliance? It is arguable. The average person certainly knows that classified data cannot be simply discarded in a public trash receptacle. But, the average layperson is unaware that destroying a computer printout does not protect the data stored in the computer memory.

Clearing memory can be difficult, and deleting a computer file

\(^{136}\) \textit{Cf. supra} notes 106-08 and accompanying text.

\(^{137}\) \textit{See supra} text accompanying notes 45-51.

\(^{138}\) The user thinks he is “moving” the data from one medium to another. What he is actually doing is “copying” the data. This is what makes theft of data different from theft of tangible items. If one “steals” a mailing list file, the organization from which it was stolen still has the original data file.

\(^{139}\) \textit{See} HOFFMAN, \textit{supra} note 4, at 93-34.
does not necessarily mean that the data is obliterated.\textsuperscript{140} There are two reasons for this. First, unbeknownst to the terminal user, the computer system may be making a backup of the terminal input for perfectly legitimate reasons.\textsuperscript{141} Therefore, even though the user has “deleted” the data, it is simply saved elsewhere. Second, a “deletion” might not physically remove the data, but only mark it as “unusable” for the present and physically remove it only upon “reorganization” of the disk. On the one hand, this improves the efficiency of the computer system, but, it also creates a risk of unauthorized access and abuse. Would management be negligent if data which has been “deleted” nevertheless managed to appear and cause harm to an individual?\textsuperscript{142}

Therefore, even if one has authentication methods which guarantee that no one can assume another’s identity, and even if one has authorization methods which guarantee that only authorized users can read a given file, there is still no guarantee that the data on the file can be restricted to authorized users. The problem, once again, is that there are no standards to specify precisely what “authorization” means.

\textit{b. Bypass Mechanisms}

Even if the problem of sensitive residue were solved, current authentication methods are still inadequate to guarantee the protection of data. The previous discussion of authorization\textsuperscript{143} implied that authorization tables, if accurately established and not circumvented by user impersonation, would prohibit unauthorized users from accessing files in auxiliary storage. However, all systems permit “bypass” mechanisms.

A bypass mechanism simply instructs the operating system to override anything specified in the authorization tables. A security


\textsuperscript{141} A backup will be appreciated if the system “crashes” and all your input would otherwise be lost and have to be tediously recreated. Crashes are not uncommon, and taking backups has been standard in the computer industry for decades.

The taking of backups turns out to be fortunate for another reason, as a major protective device against the current popular evil, computer viruses. See, e.g., C. Winter, \textit{Viruses Threatening Era of Computer Freedom}, Chicago Tribune, Feb. 21, 1988, § 7, at 1,8. It is undoubtedly true that good computer practice will remain useful in combating problems unknown at this writing.

\textsuperscript{142} The Time article quotes internationally-known computer lawyer Susan Nycum as stating, “This [situation] has worried me for years.” P. Elmer-DeWitt, \textit{id}. The irony is that if “this situation” has been known for years, why is it not common knowledge among the unfortunate public that uses computers?

\textsuperscript{143} See supra § III-D-3.
audit may indicate that the tables themselves are correct, but it will not show that they have been overridden in particular cases.

The rationale for bypass mechanisms is a technical one and is grounded, ironically, in the desire for security. All computer manufacturers realize that certain system functions must be restricted against the general run of users.\textsuperscript{144} However, on occasion, a general user has a perfectly legitimate need to use a restricted function. To solve this problem, bypass mechanisms are created, whereby ordinary users can be permitted to use restricted functions.

Permission generally comes in the form of special system codes installed by a technical programmer and given to the user.\textsuperscript{145} Yet, a large organization seldom controls its technical programmers and special codes adequately. Thus, it may not be overly difficult for an interloper to gain access to bypass codes. These codes might allow the user to access any system file, and ensure that the authorization tables were simply \textit{ignored} in the particular user’s file access decisions.\textsuperscript{146}

\begin{itemize}
  \item Three common examples of functions prohibited to general users are: the ability to rename files in auxiliary storage (which could wreak havoc for the user who could no longer find his file); the ability to change operating system code supplied by the manufacturer (known as “zapping,” this could decommission the entire system); the ability to update the system activity log (which could destroy any integrity in the monitoring and surveillance process).
  \item For example, the user may be given a code to enter over the terminal. Or, his ID may be recorded on a special operating system file of privileged ID’s.
  \item See R. Paans and I.S. Herschberg, \textit{How to Control MVS User SuperVisor Calls}, Computers & Security, March 1986, at 46. Here is a highly-condensed summary of this superb article for those interested:
    \begin{enumerate}
      \item Many systems have a fair degree of security, as delivered by the manufacturer to the user. But this security can be damaged by local modifications. The ability to modify cannot be prevented due to current market realities.
      \item IBM, the world’s largest computer manufacturer, markets the Multiple Virtual Storage (MVS) operating system. MVS is among the most secure operating systems for commercial applications in the world. It is used in the great majority of large commercial computer installations. Yet, it is vulnerable to bypass.
      \item There are two classes of computer programs running on MVS: authorized and unauthorized. Roughly speaking, unauthorized programs are equivalent to application programs (\textit{see supra} note 51 and accompanying text), and authorized programs are equivalent to O/S common routines (\textit{see supra} note 52 and accompanying text).
      \item Only authorized programs can execute restricted system functions, such as input/output operations (e.g., the ability to read from and write to files on auxiliary storage), compress disk space (for productivity reasons), and change O/S internal routines (which can include authorization table codes), etc.
      \item However, nearly all unauthorized (application) programs require the \textit{use} of restricted functions. For example, an application program may legitimately wish to read a file on a disk pack, but input/output operations are restricted functions. To get around this, MVS provides the SuperVisor Call (SVC) mechanism, which permits unauthorized programs to execute restricted functions in a \textit{totally secure} manner. The application program issues a coded instruction which causes an SVC to be executed. MVS provides over 100 “standard
It is difficult to develop cost-effective means to totally prevent bypass exposure. Although there are a variety of administrative mechanisms which could bring the exposure under control\(^\text{147}\), they are labor-intensive and tedious, and are often considered by management to interfere with the "productive work" of an installation.\(^\text{148}\)

No one would think much of a bank alarm system which could be deactivated by the flick of a switch inside an unlocked desk. Similarly, the value of an automated computer security system must

---

SVC's which permit application programs to function while ensuring security in the use of restricted system functions.

\(^{6}\) The installation is also permitted to write its own SVC's which, when invoked, allow a program to execute restricted functions. These are known as "User SVC's." The problem is that User SVC's, unlike standard SVC's, are not guaranteed to be totally secure. If used improperly, they can cause all security mechanisms to be bypassed.

\(^{7}\) User SVC's have many legitimate uses from a performance/convenience point of view. They are installed by system programmers whose primary responsibility is performance, not security. User SVC's have been found which permit unauthorized programs to defeat any type of access control. The article details several horrors, all of which are quite technical, although very easy for a systems programmer to understand. The point is that manufacturers supply mechanisms which enable qualified persons, in the name of efficiency, to defeat all known security mechanisms.

\(^{8}\) Hackers can, with talent, patience, and a little luck, find the memory address of User SVC routines. They can then use these routines in their own programs to disable security and crack the system.

\(^{9}\) In summary, an access control system is only as good as the operating system in which it functions. If the operating system allows uncontrolled User SVC's, as MVS does, then it can be secured only if it employs sophisticated, costly, labor-intensive administrative/audit checking mechanisms. Most managers would be surprised to find how vulnerable their computer systems are. In operating systems less secure than MVS, the picture may be even worse.

\(^{147}\) See, e.g., IBM, OS/VS2 System Programming Library: Supervisor, at 23-27 (1985). In the case of User SVC's some recommended controls include: ensure that User SVC's, are implemented only in accordance with strict guidelines developed and supervised by technical, security and audit staff; ensure that User SVC's are tested by persons other than the developing programmer; ensure that User SVC's cannot be accessed by "unauthorized" programs (see supra note 144, \#3); since authorized programs reside in authorized libraries (groups of programs), determine what these libraries are and who controls their usage.

The problem is that there is no general test to ensure that security is not compromised by User SVC's or other bypass mechanisms. There are so-called "MVS Audits," which purport to check the integrity of MVS security. Such audits, if properly performed, are very expensive and tedious. The enforcement of their recommendations is usually left to the very technical staff against whom they were directed. Of course, no standards require MVS audits to be performed by competent and disinterested parties in the first place.

\(^{148}\) The author recalls one particularly horrifying experience in which he thought he was administering security in a medium-size computer system, while at the same time the manufacturer's local representative (not IBM) was instructing clerical users in an easy method to bypass the security system! The representative had made one promise to the author and another to the line manager. The author discovered this, quite by accident, thanks to the keen ear of his senior subordinate. She was friendly with a clerk who inadvertently let the matter slip out, not unlike the discovery of the existence of the Oval Office tapes.
be measured, at least in part, by the ease with which it can be overcome. Standards are required to define the acceptable limits of bypass mechanisms and controls thereon, and to be reasonably certain that access control software is adequate to protect data against anyone other than computer novices.

c. Lack of Uniform Security Architecture

If the problems of sensitive residue and bypass mechanisms were solved, one might suppose that access control software would effectively prevent unauthorized users from accessing another's data. That might be true if, as previously implied, the access control software actually covered the entire computer system.

But such is not the case. What appears as "the computer system" is, in reality, a group of several different hardware and software sub-systems. The problem is that access control software is neither hardware-independent nor software-independent. This means that access control software which runs under one version of hardware and software will not necessarily run if that hardware or software is altered. Thus, adding a technical enhancement to the computer system to increase productivity may destroy existing security mechanisms or render them far more difficult to use effectively.149

Again, the reason for this anomalous situation is the concern for security. Many software subsystems were developed before any general software security existed. Therefore, enlightened software engineers developed their own subsystem controls. When general access control software security packages came into their own, the existing subsystem controls were not merged in due to cost factors. Instead, a mixture of uncoordinated, incompatible, incomplete, and redundant controls coexisting in the same computer systems

---

149. As technology has advanced to meet [business] demands of automation[,] emphasis has been placed on performance and productivity. Although many data processing controls are administrative and procedural, rather than automated, there has been a lack of emphasis on automated controls being integrated with new technology. The scope and quality of the automated controls that have been incorporated have not been independent of the environment in which they are used (i.e., hardware, software, or configuration).

Directions, supra note 133, at 3 (emphasis added).

In former days, a version of COBOL might run on one machine but not on another. Cf infra text accompanying notes 191-92. In industry jargon, COBOL was not hardware-independent. Today it is, but access control software is today neither hardware-independent nor software-independent. Thus, a change of hardware or software in the computer system can and often does render the security system inoperable.
emerged\textsuperscript{150}, and no one was willing to overhaul the whole system to ensure coordinated controls.

The obvious technical solution is a "uniform security architecture"\textsuperscript{151}. Security would no longer be an "add-on" to the operating system\textsuperscript{152}, but an integral part of the operating system itself.\textsuperscript{153} However, it makes no sense for one manufacturer to spend itself into bankruptcy attempting to construct the perfectly coordinated system, while others continue to successfully compete with uncoordinated add-on packages.

Since there are no computer security standards for new products, it is impossible to fault manufacturers for responding to perceived market demands.\textsuperscript{154} Therefore, corporate officers and directors may proudly point to sophisticated access control software which "ensures" security and privacy, while ignoring the fact that hardware and software additions can easily destroy what vestige of security had been present.

Access control software, as it exists today, offers very little guarantee of computer security. Protection against retrieving another's files can be bypassed in a virtually uncontrolled manner. Even if files are secured, the data thereon is not and may be retrieved from the main memory. Finally, since there is no uniform security architecture, the existing security mechanisms themselves may be rendered meaningless by add-on hardware and software. These facts are well known in the industry and among practitioners, but because they pose formidable technical and financial problems, they are largely ignored.

3. Ensuring Individual Privacy in Statistical Data Banks

The public often perceives security in numbers, feeling more

\textsuperscript{150} See Directions, supra note 133, at 3-4; Response, supra note 134, at 3-6. As one example, attaching personal computers to a large computer system may subvert the controls on the large system. Directions, supra note 133, at 4; Response, supra note 134, at 6.

\textsuperscript{151} "[A] uniform security architecture must be provided such that all [hardware and software] sub-systems are able to be supported by the architecture and security system." Directions, supra note 133, at 3.

\textsuperscript{152} "[T]he term 'security package' is something of a public disgrace for the industry. In any proper industry, it should not exist. Security, if industry is to deliver a satisfactory product, should be part and parcel of an operating system... there should be no such thing as a security package. . . . option with all its attendant fees and complications. It should be an integral part of normal operations. . . ." Herschberg, supra note 125, at 137.

\textsuperscript{153} In other words, computer security would be a "common routine" that could not be subverted by individual users. See supra note 52 and accompanying text.

\textsuperscript{154} Cf. supra note 134.
protected by statistics than personal information. For example, suppose a husband publicly accuses another of wife-swapping. Because a jury could easily identify the person accused, it would have no difficulty finding the husband guilty of defamation. However, suppose the husband publicly accuses ten unidentified men in a group of one hundred. Since the public would have difficulty perceiving which ten of the one hundred were guilty of the alleged impropriety, a jury would probably find no liability.

Consider the comments of Theodore Hesburgh, former president of the University of Notre Dame and former Chairman of the Select Commission on Immigration and Refugee Policy. In discussing the virtues of a national ID card as a method for keeping illegal aliens from employment in the U.S., Hesburgh briefly mentions the national data bank that would be necessary to support the card.\textsuperscript{155} To allay fears of the data bank's security, he advises that "[u]se of numbering systems rather than names in central data banks would shield the individual's privacy behind anonymity."\textsuperscript{156}

Although it makes sense that one is harder to identify in a group, this same assumption cannot be made with regard to computerized data banks. It is not necessary to know personal identifying information to deduce a person's identity mathematically from surrounding facts.\textsuperscript{157} Consider Hoffman's standard example. Ask the hypothetical national statistical data bank how many persons were born in Omaha, in 1913, are members of Phi Delta Phi, have lived in Alexandria, Virginia, graduated from the University of Michigan, and are Episcopalians. If the answer comes back "1", then you have isolated President Gerald Ford, using easily obtainable public data and having committed no crime. If you now ask how many persons, in addition to the above qualities, have been convicted of a crime, the answer will come back "0" or "1", revealing whether or not Gerald Ford has been convicted of a crime.


\textsuperscript{156} Id.

\textsuperscript{157} Even if the [data base] system . . . doesn't even contain any identifying information . . . it is possible to obtain a personal dossier on that person from such a data bank. The potential for such use is often not obvious to users, especially nontechnical users, of computers. They assume incorrectly that deletion of names or other identifying information will guarantee the privacy of people whose records appear in such data banks. This is not necessarily true.

L. HOFFMAN, \textit{supra} note 4, at 124.

Note also that privacy can be invaded by less imposing data banks. For example, marketing firms and banks that possess census tapes with block (neighborhood) data have the potential to discern personal information.
This information is obtainable despite the fact that the hypothetical national statistical data bank does not contain personal identifying information on Mr. Ford (i.e., no name, no social security number, no address, etc.). This same information can be obtained if the system returns even large counts of the number of persons who qualify.

Suppose that an individual's privacy were invaded by dissemination of information garnered from a statistical data bank. Could the individual claim that the data base manager had been negligent if there were no personal identifying data in the data bank? Some may not even recognize the existence of that question. Others may maintain that the data base manager, by supplying no personal data, is not responsible for any damage.

There are several possible solutions to this problem. One method is to "inoculate" the statistical data bank with random errors. If done carefully on certain types of files, the inoculation would preserve statistical validity and protect individual anonymity. Another method is to report inexact counts of persons. For example, a range of persons (e.g., 20-30 persons with these characteristics) could be reported, or an indication made that "a small number" (e.g., less than ten persons with these characteristics) was found. This method, however, is not foolproof; nonetheless, it will add a degree of protection for individuals. Another method, valid more for psychological than practical reasons, is to let users know that all requests for information from the statistical data bank will be logged.

Again, the underlying problem in protecting personal information in statistical data banks is that there are no standards specifying what administrative and technical measures must be taken to ensure individual privacy. Yet measures to ensure a reasonable level of security have been known for years.

4. Miscellaneous Issues

There are several additional areas in which the installation of a
computer security package alone offers no guarantee of protection. These are listed below, with minimal detail.

a. **Electronic Mail**

Businesses are increasingly using electronic mail systems to improve productivity and efficiency. Rather than waste time on the telephone or at the copy machine, a user can send a personalized message over the terminal to another individual or copies of memos to several terminals simultaneously.\(^{163}\)

When an individual receives a message through the mail, the terminal normally will show the name of the sender, based on the ID-Code and password the sender entered to sign on to the system in the first place. Of course, knowledge of the identity of the sender is only as good as the security of the password. Typically, electronic mail passwords are far less secure than passwords in access control software systems.\(^{164}\)

The result is a problem for offices which wish to rely on "automated signature authentication" (i.e., the sender's ID as shown on the terminal) rather than the customary physical signature. A good authentication technology, therefore, would not only help in proving identity for access control software, but would also have a beneficial effect on office automation and productivity.

b. **Violation Reporting**

It is generally accepted that security systems should not merely prevent unauthorized access, but should assist system administrators in tracking down potential violators.\(^{165}\) Yet, many systems report violations in "batch" mode (i.e., hard-copy reports given the next working day to an administrator) rather than "real-time" (i.e., notice given at a security console when the violation is occurring). Furthermore, many systems cannot disable an ID during an attempted violation (i.e., three password errors in a row), or disable a terminal where violations are occurring. It is as if a bank teller pressed a burglary alarm during an attempted but unsuccessful rob-

\(^{163}\) Any receiving user can get a hard-copy at his unit's printer if he really needs it. It is surprising how seldom that turns out to be necessary.

\(^{164}\) One of the most popular electronic mail systems in use today offers only a 3-position password, with no restriction on its values, and no mechanism to enforce mandatory password changing. This is understandable: the idea of large system security is generally acknowledged if not always practiced; but electronic mail system security has not achieved that degree of user sensitivity as of this writing, probably because it offers less opportunities to outside "hackers" than does a large system.

\(^{165}\) See supra § III-D-4, 5.
bery on Friday, but because of infrequent monitoring, the police did not get the signal until Monday morning. This situation makes it far less likely that an intruder will be caught, and far more likely that he will continue to try to gain unauthorized access until he succeeds in disrupting the system.

Also, the violation reports that are produced are often cumbersome or unusable for system administrators. They may feature too much detail, or not enough, and generally lack the required flexibility to produce specific details on demand. The reason is that reporting mechanisms are driven by convenience to system designers who have added security after-the-fact\textsuperscript{166}, rather than by convenience to security personnel who are responsible for ensuring protection of sensitive individual and company data.\textsuperscript{167} If a hacker whose activities were detected but who has nonetheless remained undisturbed eventually causes harm, can it be said that the organization was not negligent simply because it had some semblance of a violation reporting mechanism in place?

c. Administrative Methods

Administrative security controls are often regarded as secondary to technical security controls. They neither prevent nor report unauthorized access, but simply support the systems which do. Administrative controls are not generally manufactured and marketed nationally but are created internally within the organization. Finally, they are typically implemented by persons paid less than those who implement technical controls. It is not surprising that even persons who favor technical computer security standards seldom feel compelled to speak in favor of administrative computer security standards.

\textsuperscript{166}. See supra notes 149-54 and accompanying text.

\textsuperscript{167}. See Directions, supra note 133, at 9-10, for an indication of violation report needs generally un-met today. These include: flexibility in report selection criteria; more helpful data in tracking down violators; deletion of overly-friendly messages that could help system abusers.

Lack of standardization will cause a problem when attempting to document precisely what happened during an attempted security violation. Discussing the efficacy of computer crime laws in prosecuting offenders, Gerard Marsh, a computer security vendor executive, notes that “The catch is that [for prosecution], the perpetrator's actions have to be documented, placing the burden of proof on data owners. Thus, it is advisable...[to] have adequate software security products installed which can generate accurate and complete audit trials...The problem here is that all [products] operate differently.” Marsh, Computer Crime Law Makes Software Safeguard Vital, INFORMATION WEEK, Feb. 2, 1987, at 40 (emphasis added).

The general vendor answer to these needs is that the cost is greater than what the market will bear. Response, supra note 144, at 10.
Yet, administrative standards are important. An individual might be assured by the company holding his data that it performs "security education and awareness" programs for its employees to ensure the proper level of attention to security concerns. An individual should have some understanding of what "security education and awareness" means in order to meaningfully evaluate the effectiveness of the program. However, there is very little published on this subject, and individuals seeking to develop standards and evaluate effectiveness will have to fend for themselves.168

Similarly, an individual might be assured that the company holding his data has a "contingency plan", to assure that information can be recovered reasonably quickly and completely in the event of a data center disaster. The individual should have some understanding of what this means, and an assurance that the plan is tested and maintained. Again, there are no standards by which timely and accurate recovery are generally measured.169

168. See, e.g., B. WILKINS, THE INTERNAL AUDITOR'S INFORMATION SECURITY HANDBOOK 44-46 (1979); Agranoff, supra note 91. Briefly, desirable practices include, but are not limited to: existence of a separate computer security unit; publication and regular maintenance of a security policies and procedures manual; regular security presentations to staff; routings to selected managers; placement of appropriate items in house organs; design of forms which double as security procedures for busy operating management; orientation sessions for new employees; separate company phone listings for Security; establishment of a team to quickly respond to computer crime situation; and, occasional lectures by guest speakers.

169. The author personally knows of an agreement a few years ago among three local companies to make their data center available in case one company had a disaster. The agreement was abandoned when one company suggested it be tested. So many modifications in each company's systems had been made over the years that no company's software could run on the other's hardware and version of the operating systems.

More recently, it is reported that nearly half the insurance companies responding to a survey stated that they had no written disaster recovery plans, and 40% of those that have such plans have never tested them. COOPERS & LYBRAND EXECUTIVE SUMMARY, COMPUTER SECURITY IN THE INSURANCE INDUSTRY (1987). For more information, the reader is referred to the local Coopers & Lybrand office. For a detailed discussion of computer disaster recovery see Burk, Failure to Prepare: Who's Liable in a Data Processing Disaster, 5 S. C. COMPUTER & HIGH TECH. L.J. 19 (1989).

It is further reported that no more than 50% of banks are prepared adequately to deal with disasters. Baker, A New Verdict on Disaster Recovery, COMPUTERS IN BANKING, Nov. 1987, at 69, 76.

Banking senior management and their boards of directors have been put on notice that they are responsible to assure the existence of adequate plans to minimize risk to their institutions. This should foster the support of senior management that is often the lacking element at financial institutions. If the printed words do not, then the comments of examiners [backed by FHLBB Memorandum R67, issued Sept., 1986] should cause action. Id. at 81.

The testing of contingency plans, and follow-up thereto, is among the most tedious activities that a large organization may engage in. The temptation to "skimp" on necessities is too
Administration is a broad topic which cannot be completely discussed here. The point to emphasize is that the existence of "administrative controls" means virtually nothing. There are no standards for evaluating the effectiveness of a given administrative control relative to the technical control that it supports. However, the implementation of meaningful technical standards should also pave the way for the eventual establishment of meaningful administrative standards.

IV. Protection of Society: The Need for Meaningful Federal Computer Security Standards

The previous sections have examined computer system fundamentals, computer security fundamentals, and implementation problems. Liability to persons injured as a result of unauthorized access to computerized data depends, in part, upon the accepted standards of protection for that data. The problem is to translate computer security principles into meaningful standards which will permit compensation to computer abuse victims and help to reduce the incidence of computer crime.

A. Differing Views on Developing Standards

Much has been written on the need for standards in the computer field. However, few offer suggestions as to how these standards are to be developed. One attorney believes standards should be developed on a case-by-case basis, allowing a jury to decide the correct standards to be used in a particular fact situation. However, with the enormous variations in computer applications and security practices today, a jury is likely to be confused and may even want written standards to ensure individual justice. In response to a query from the author, the attorney responded that the area is "too new" to allow for meaningful standards.

Fortunately, many lawyers are aware that individuals and society in general are victimized by the lack of standards of due care for the protection of computerized data and that standards are unlikely to develop on their own. Several recent law review articles have recognized that establishing tort liability for information processors might be necessary to protect the public. In reviewing various

obvious for comment. It is the author's personal opinion that adequacy of a company's contingency plan should not be assumed unless certified by competent, qualified, disinterested outsiders.

170. See supra notes 88-94 and accompanying text.
threats to personal privacy that are exacerbated by computers\textsuperscript{171}, one article states, “[t]he processor would be liable for any breach of due care, which would... be judged against standards of an ordinarily prudent person within the industry and under similar circumstances.”\textsuperscript{172} But how does an “ordinarily prudent person within the industry” act? The article did not provide specifics, but only noted that because of the inadequacies of current security measures, businesses might be “forced” into executing protective measures.\textsuperscript{173}

Another article considered the harm that could be caused by persons using electronic bulletin boards.\textsuperscript{174} For example, malefactors can use electronic bulletin boards (EBBs) to steal proprietary software, circulate stolen credit card numbers, and even operate illegal businesses.\textsuperscript{175} The article suggests that although the message originator actually causes the harm, the EBB operator should be liable if necessary “both to discourage misuse and to reduce the damage resulting from it.”\textsuperscript{176} However, liability should only be imposed if the bulletin board operators acted unreasonably by failing to take certain precautions generally accepted within the industry.\textsuperscript{177} It is unlikely that a court would find a law review article’s standards dispositive. More likely, a court would note that no generally-accepted industry-wide standards of due care currently exist.

Although each of the above articles suggests standards for evaluating computer negligence, each suggests that these standards should be developed on a case-by-case basis, according to developing public acceptance of their use. However, victims of computer abuse should not have to wait for the common law to develop in each of the fifty states, particularly since computer technology is developing across state lines at such a fast pace. Common law standards are likely to be obsolete before they are implemented. Mandatory federal regulations are needed.


\textsuperscript{172} Id. at 789.

\textsuperscript{173} “Technological security must be purchased and so far there has been no profit motive in the industry to provide security systems. As the computer is used more in privacy sensitive areas, the industry should be forced to realize that it is making a potentially dangerous product and, like the automobile manufacturer, the industry should be expected to take responsibility for providing the necessary safety features.” Id. at 786.


\textsuperscript{175} Id.

\textsuperscript{176} Id. at 445.

\textsuperscript{177} Id. at 452.
B. Response of the Organized Bar

The American Bar Association has promulgated a report in response to the need to combat computer crime.\textsuperscript{178} Although the report recognizes the inadequacies of current security measures, it fails to consider the underlying technical issues.

In preparation of the report, the Criminal Justice Section of the ABA appointed a task force to investigate various approaches organizations took to combat the problem.\textsuperscript{179} The task force sent a ten-page questionnaire\textsuperscript{180} to executives of large corporations, major federal agencies, all state attorneys general, and some district attorneys.\textsuperscript{181} The task force stated in its cover letter that response should take no more than 15 to 20 minutes.\textsuperscript{182} However, the questionnaire contained several hundred individual items, many of which were argumentative and ambiguous, or required considerable investigation. Thus, a 15-20 minute time period is unlikely to have elicited responses necessary to formulate public standards.

Despite the report's shortcomings, it correctly concludes that federal computer crime legislation is needed\textsuperscript{183}, and advises lawyers that until legislation is passed, better computer security measures are needed to deter computer crime.

Regardless of these recommendations\textsuperscript{184}, though, the task force has done nothing to implement action. The task force has even refused to indicate if it will ever take any action. In short, despite its enormous prestige, the task force has done nothing to help lower the technological gap.

Perhaps one of the reasons the task force has failed to act is its lack of technical qualifications to deal with the problem. Although few attorneys are truly qualified to develop standards to combat computer crime, the interests of persons who have been injured by computer abuse are ill-served by lawyers who have no understanding of the underlying technology or of the need for standards.

\textsuperscript{178} See A.B.A. Report, supra note 37. The A.B.A. Report was cited by Congress as “one of the first extensive studies done on the number of ‘known and verifiable losses’ which have resulted from computer crimes . . . .” H. R. REP. No. 153(1), infra note 211, at 9. It has been cited in trade journals too numerous to mention.

\textsuperscript{179} Kuh & Nathan, Preface to A.B.A. Report, supra note 37, at iii [hereinafter Preface].

\textsuperscript{180} A.B.A. Report, supra note 37, at I-2 to I-12.

\textsuperscript{181} Preface, supra note 179, at xi.

\textsuperscript{182} A.B.A. Report, supra note 37, at I-1.

\textsuperscript{183} Id. at 45-51.

\textsuperscript{184} Preface, supra note 179, at xv.
C. Corporate Management Response

Much material published on computer security castigates corporate management for not doing more to implement computer security. Yet the simple fact remains that computer security is not currently considered economically feasible. Top management emphatically is not equipped to ferret out individual rights deemed worthy of protection and establish mechanisms to effectuate them. Rather, lawyers and legislators should take the lead in urging that standards be created.

In this regard, corporate management is trapped by conflicting pressures, desiring both high security and low cost. Both cannot be provided. Thus, although managers may give lip service to security, they are unable to economically afford it. However, if mandatory federal security standards were established, middle managers could justify cost to upper management without sacrificing competitiveness. As a result, business would be forced to invest in computer security without losing their competitive advantage to other computerized companies since each would be adjudicated by the same standards. The businesses would benefit in remaining competitive and the public would benefit from better protection from computer abuse.

D. Congressional Response

1. The Recognition

The case for mandatory federal computer security standards was first articulated by Dr. Willis H. Ware. Dr. Ware, a computer security pioneer, reviewed the need for computer security in government and private industry, noting that several federal stan-

185. No responsible management is going to spend large amounts of money with no tangible payoff in sight, and without legal compulsion to do so, the protests of staff analysts notwithstanding. As one authority crisply stated, "Senior management interest rarely lasts long when dealing with non-profit-center functions." Johnston, The People in the Black Hats, INFOSYSTEMS, Sept. 1987, at 35. To look at the situation concretely: Would management spend millions of dollars on fire-resistant buildings if it didn't have to, and if in so doing it would price its company out of the market?

186. P. KEEN, COMPETING IN TIME: USING TELECOMMUNICATIONS FOR COMPETITIVE ADVANTAGE 129 (1986). Dr. Keen has taught at Harvard, MIT, Stanford, and Wharton.

187. Ware, supra note 33, at 71. Dr. Ware's brilliant article was the inspiration for this present paper. Dr. Ware participated in the first serious consideration of computer security in 1967, and among other things, spent two years with the Privacy Protection Study Commission.
standards related to computer security already existed.\textsuperscript{188} He asked, "[w]hy not, under the auspices of [the National Bureau of Standards], bring together the best resources within (and from outside) government to handle the remaining details of security safeguards?... Why not have [standards which] specify the performance requirements of a secure operating system plus the administrative, procedural, and physical elements in which it has to be embedded?"\textsuperscript{189} Many computer security professionals would favor standardized controls if they saw no other way to achieve the necessary standards of control.\textsuperscript{190}

The question is not so much whether government action is needed, but whether there is an alternative. In the early 1960's, recognizing that a standardized business programming language would be highly desirable, the federal government pressured private industry to develop COBOL. This became a United States standard in 1968 \textsuperscript{191}, and today is used extensively by private industry with no ill effects. Without government action, financial considerations would have prevented the standardized development of COBOL, just as these considerations prevent the development of standardized computer security controls today.\textsuperscript{192}

Attorney Daniel Burk, a distinguished attorney who drafted the computer crime statutes for Virginia and the District of Columbia\textsuperscript{193}, recognizes the "strong interdependence among technical, legal, and managerial approaches" in the fight against computer crime\textsuperscript{194}, and encourages legislation which implements "the concurrent use of technical and managerial solutions."\textsuperscript{195} While he stops short of stating that these solutions would also assist in securing compensation for victims of computer abuse, that is clearly the next step. Technical standards are necessary to solve computer abuse, and "technical solutions" should not be left to the whims of corpo-

\begin{itemize}
\item \textsuperscript{188} Id. at 76. These include the Data Encryption Standard (DES) and certain Federal Information Processing Standards (FIPS), which are largely administrative.
\item \textsuperscript{189} Id. at 76.
\item \textsuperscript{190} Legally, the bottom line for failure to secure a network which results in data destruction or corruption, may well be negligence. ... Stockbrokers, customers, and other interested parties may see themselves as the victims. ... When the legal world meets the computer world the latter can discover that it has not covered bases well enough to satisfy the former. \textsc{Datapro Research Corp.}, \textit{Datapro Reports on Information Security} IS35-200-106 (1985).
\item \textsuperscript{191} Shelly & Cashman, supra note 33, at 13.5.
\item \textsuperscript{192} See supra notes 185-86 and accompanying text.
\item \textsuperscript{193} \textsc{Computer Systems}, supra note 16, at 171.
\item \textsuperscript{194} Id.
\item \textsuperscript{195} Id. at 174.
\end{itemize}
rate and vendor management since past experience has shown that voluntary action is unlikely. 196


The Computer Security Act of 1987 (the "1987 Act"), which became effective January 8, 1988 197, states that "improving the security and privacy of sensitive information 198 in Federal computer systems 199 is in the public interest ... ." 200 Its major purpose is:

to assign to the National Bureau of Standards [NBS] responsibility for developing standards and guidelines for Federal computer systems, including responsibility for developing standards and guidelines needed to assure the cost-effective security and privacy of sensitive information in Federal computer systems. ... 201

NBS is to submit these standards and guidelines to the Secretary of Commerce who may promulgate them as compulsory and binding under authority of the Federal Property and Administrative Services Act. 202

If the 1987 Act results in the development of meaningful computer security standards for the Federal Government, then it is likely that these standards would gravitate to the private sector. The Federal Government is the world's largest computer user. 203 Any significant computer security standards which vendors must meet in selling to the Federal Government would require considerable hardware and software subsystem changes. 204 These changes would likely find their way into the very subsystems which vendors sell to private industry. 205

Therefore, the question is whether the 1987 Act will eventually result in meaningful computer security standards, i.e., standards which will eliminate or reduce the problems in computer security

196. "[T]echnical restraints may require the sanction of law both to act as an additional deterrent and as a method of 'blessing' technical restraints in general." Id.


198. "Sensitive information" is broadly defined to include any information whose misuse "could adversely affect the national interest or the conduct of Federal programs. ... ." Id. at § 3.

199. "Federal computer systems" are broadly defined to include virtually any computer operated by or on behalf of a Federal agency, except for defense and military intelligence systems. Id.

200. Id. at § 2.

201. Id.

202. Id. at § 4.

203. See SHELLY & CASHMAN supra note 33.

204. See supra notes 149-53 and accompanying text.

205. Id.
previously noted.\textsuperscript{206} If so, then the dawn of computer security protection for individuals and businesses is on the horizon\textsuperscript{207}; if not, then the "charade of computer security" will continue.\textsuperscript{208}

The 1987 Act specifically assigns NBS the responsibility for developing computer security standards and guidelines in all areas (technical, physical, administrative)\textsuperscript{209}, and authorizes NBS to conduct research to determine computer data exposures and devise cost-effective controls.\textsuperscript{210} The accompanying House Report specifically recognizes that the Institute of Computer Science and Technology (ICST) within NBS already has a good track record in standards development.\textsuperscript{211} NBS is further assigned supporting responsibilities, such as development of security awareness and practice guidelines to be used by Federal agencies,\textsuperscript{212} and advisory authority on computer system security and privacy plans which Federal agencies will be required to establish.\textsuperscript{213} In other words, Congress appears to be taking the purpose of the 1987 Act seriously.\textsuperscript{214}

There is a danger sign, however. Immediately after acknowledging that the 1987 Act would influence the private sector, the House Report added that "NBS should consider the effect of its standards on the ability of the U.S. computer system manufacturers

\begin{itemize}
\item \textsuperscript{206} See generally supra § III-E.
\item \textsuperscript{207} "H.R. 145. . .standards and guidelines will strongly influence security measures implemented in the private sector." H.R. REP. NO. 153(I), supra note 211, at 27.
\item \textsuperscript{208} Cf. supra note 152.
\item \textsuperscript{209} 1987 Act, supra note 197, § 3.
\item \textsuperscript{210} Id.
\item \textsuperscript{211} H.R. REP. NO. 153(I), 100th Cong., 1st sess. 6 (1987).
\item \textsuperscript{212} Computer Security Act of 1987, Pub. L. No. 100-235, § 5, 101 Stat. 1725 (1988). Federal agencies will be required to implement the programs in a timely manner prescribed by the Director of the Office of Personnel Management. Id. at § 6.
\item \textsuperscript{213} Id.
\item \textsuperscript{214} [The Computer Security Act of 1987] would give the National Bureau of Standards — not a military agency — the responsibility to assess the vulnerability of government computer and information systems except for critical defense and intelligence systems. [It] will put new emphasis on the need for developing increased awareness of the importance of computer security and on the potential losses or disruption of vital government programs that could result from unauthorized access to Federal computers.
\end{itemize}


For an account of the modest struggle between NSA (military) and NBS (civilian) over which agency would control computer security standards for unclassified data, see 133 Cong. Rec. H5341-44 (daily ed. June 22, 1987); H.R. REP. NO. 153(I) 100th Cong., 1st sess. 7-22 (1987). Both sides, military and civilian, did in fact favor the establishment of federal standards.
to remain competitive in the international marketplace."\textsuperscript{215} Although this statement may merely acknowledge the high cost of re-tooling hardware and software sub-systems to effectuate meaningful computer security, it may give manufacturers the ability to "gut" the 1987 Act.\textsuperscript{216}

3. The Prospects

Although the 1987 Act was signed by the President on January 8, 1988 \textsuperscript{217}, no Board members\textsuperscript{218} were appointed until December 12, 1988.\textsuperscript{219} The Board held its first meeting March 1-2, 1989,\textsuperscript{220} and plans to hold its next meeting May 31-June 1, 1989.\textsuperscript{221} As of May 8, 1989, the Minutes of the March meeting were not publicly available.

The composition of the Board itself is somewhat disturbing. Four members are appointed from the Federal Government, four from the computer industry, and four from outside the Federal Government not employed by the computer industry.\textsuperscript{222} It may be assumed that the Federal Government representatives favor the establishment of meaningful computer security standards.\textsuperscript{223} It may also be assumed that the computer industry representatives will be attuned more to commercial market conditions that to the need for

\textsuperscript{215} H.R. REP. No. 153(I), 100th Cong., 1st. sess. at 27 (1987).
\textsuperscript{216} The Computer Security Act of 1987 envisions the creation of the Computer System Security and Privacy Advisory Board (the "Board"). The Board consists of a Chairman and 12 members. Eight of the twelve members are from outside the federal government and receive only travel expenses for their services. Four of those eight members may be employed by manufacturers. In effect, Board members serve pro bono.

At least one of the four federal government members must be from NSA. The Board reports its findings, not solely to NBS, but also to the Secretary of Commerce, OMB Director, NSA Director, and certain congressional committees. The Computer Security Act of 1987, Pub. L. No. 100-235, § 3, 101 Stat. 1725 (1988). There is no provision for computer lawyers to be members of the Board.

According to one authority, The National Bureau of Standards plans to use the 1987 Act to develop meaningful computer security standards that would reach the private sector. Telephone interview with Dr. James Burrows, Director of The ICST (Nov. 19, 1987).

\textsuperscript{218} See supra note 216.
\textsuperscript{219} U.S. Department of Commerce News, TN-5709, Dec. 12, 1988. Note that NBS became NIST, the National Institute of Science and Technology.
\textsuperscript{223} See supra note 214.
compensation of victims of computer abuse. Thus, the balance of power may be held by the non-Government, non-industry representatives. It would seem logical for this group to be composed of "computer security professionals" working in commercial applications today. Yet, that did not happen for two reasons: first, Board members receive no compensation, making it unlikely that the best-qualified active professionals would be able to serve; secondly, it is unlikely that the best-qualified active professionals had even heard of the Board, or that the Board would have known which professionals to seek out. In short, the professionals most likely to understand the shortcomings of today's computer security systems, the persons forced to deal with these systems on a day-to-day basis and without a vested financial or political interest in the systems, have been excluded from the Board.

The Board, of course, is solely an advisory body. One might suppose that its findings would be reported to the Director of NIST (formerly NBS) who would then submit them to the Secretary of Commerce. But in fact, members of the Board can circumvent NIST by reporting directly to "the appropriate committees of the Congress." Any representative group which feels that the Board's recommendations are not in its interests can lobby its own case directly in Congress.

It is further unclear if NIST considers the development of meaningful technical computer security standards to be a high priority. NIST testimony following the March 1-2, 1989 Board meeting refers to "the development of needed voluntary industry standards." Curiously, there is no explanation as to why mandatory standards would not be sought. Stranger yet, an attach-

224. See supra text accompanying notes 133-34, and 191-92.

This comment is not intended to denigrate computer industry representatives, many of whom the author is friendly and many of whom sincerely believe that computer security must be improved. It simply recognizes the fact that manufacturers are in business to make a profit and should not and will not venture into money-losing activities without compulsion to do so.

225. See supra note 216.

226. Most computer security professionals are not lawyers, and their knowledge of the law in this area is limited to what they read in COMPUTERWORLD and other trade journals.

When the author asked Ms. Radack, supra note 220, whether he himself would be appointed to the Board, Ms. Radack replied, "It's doubtful. Have you applied?" In other words, a non-lawyer computer security professional would have to know that NBS was seeking applicants for the Board.


228. See supra note 202 and accompanying text.


The testimony heavily emphasizes NIST review of current government agency security plans. It makes clear the fact that the “turf war” with NSA is not over. Yet, it has almost nothing to say regarding private sector technical standards.

Thus, the Computer Security Act of 1987, whatever it may accomplish for NSA and NIST, may not actually result in the establishment of meaningful computer security standards to reduce or eliminate the problems described earlier. Nothing less than an adequately-funded subcommittee, with public hearings, technical and legal staff, and witnesses not bound to the computer hardware and software industry, is likely to produce the standards necessary to compensate victims of computer abuse and protect society from computer crime. Yet no public outcry for such standards has been heard, making their implementation unlikely in these days of deregulation.

V. CONCLUSION

The future is being driven by a technology so rapid that even professionals in the field have difficulty keeping current. There is virtually no chance that common law courts can protect individual rights and compensate victims of computer abuse in the face of this expanding technology. When individuals are powerless to respond, and private enterprise cannot or will not respond, then Government, guided by public-spirited lawyers, must step in with meaningful, workable solutions. Mandatory federal standards, established under authority of the Commerce Clause, are necessary to ensure protection of individuals against computer abuse. Persons who do not believe that the situation is serious enough to warrant the high

---

231. “Computer technology can itself be part of the solution to the problem of protecting computers and the data they handle.” Kammer, Attachment at 2, (emphasis added).

232. Id. at 5-8.

233. Id. at 34. See also supra note 214.

234. Dr. Willis Ware (see supra notes 187-88 and accompanying text), a member of the Board, told the author in a telephone conversation on April 14, 1989, that he did not believe that the 1987 Act would have any substantial impact on private sector computer security. An NIST staff member, who requested anonymity, told the author in a telephone conversation on April 24, 1989, that NIST “hoped” that any standards set for federal computer systems would permeate to the private sector, but that this could not be assured. In light of these comments, and action under the 1987 Act to date, it is apparent that the federal government is not interested in a uniform security architecture necessary to ensure meaningful computer security. Cf. supra § III-E-2-c.

235. See supra § III-E.
cost of standards\textsuperscript{236} might ask themselves: what will it be like by the year 2000.\textsuperscript{237}

\textsuperscript{236} For an account of what happens when Congressional action is delayed due to budgetary constraints, see H.R. REP. No. 100-1088, 100th Cong., 2nd Sess. (1988) (crisis in the nation's financial institutions caused in part by failure to maintain adequate salaries and expenses for federal regulators and law enforcement agencies).

\textsuperscript{237} This situation promises to get worse. The latest data processing buzzword, as of May, 1989, is "integration." Integration means different things to different people, but generally is understood to refer to the uniting of information technologies, i.e., data base, applications, and networks (global and local), within one company. The major integration problem is that multi-vendor (and often incompatible) hardware and software systems, which exist at nearly all large companies, must be taken into account in the unification process. See, e.g., Computer Focus on Integration, A. Dooley, ed., April 3, 1989.

Is it reasonable to suppose that technicians and users responsible for integration have made data security a priority item? In reference to what standards?

The bottom line is that integrated systems, more powerful, efficient, and user-friendly than today's "standard" systems, are the wave of the future. If it is difficult to retrofit security packages into standard systems (see supra § III-E-2-c), it will be several times more difficult, if not impossible, to retrofit security packages into multi-vendor integrated systems, if meaningful security has not been part of integration planning from the start.

Individuals may have far more to fear from the development of future commercial computer systems than they currently realize. There are no generally-accepted industry-wide security standards for integrated systems, to which enterprises might be held to account. It is as if a three-story building were expanded to twenty stories, and after expansion, someone thought to ask if the foundation were adequate to support twenty stories.

It would be preferable, the author believes, if computer security standards could be set by the private sector, just as generally-accepted accounting principles are set by the private sector. But the economics of modern technology will not allow it. The federal government must no longer hesitate to use its Commerce Clause powers to protect citizens.