Western New England Law Review

Volume 12 *12 (1990)*
Issue 2

Article 1

1-1-1990

RISK ALLOCATION FOR COMPUTER SYSTEM SECURITY BREACHES: POTENTIAL LIABILITY FOR PROVIDERS OF COMPUTER SERVICES

Cheryl S. Massingale

A. Faye Borthick

Volume 12
Issue 2
1990

WESTERN NEW ENGLAND
LAW REVIEW

RISK ALLOCATION FOR COMPUTER SYSTEM SECURITY BREACHES: POTENTIAL LIABILITY FOR PROVIDERS OF COMPUTER SERVICES

CHERYL S. MASSINGALE* AND A. FAYE BORTHICK**

When unauthorized individuals first gained access[1] to computer

* A.B., University of Tennessee; M.B.A., University of Tennessee; J.D., University of Tennessee. Assistant Professor of Business Law, University of Tennessee.

** B.S., University of Tennessee; M.B.A., University of Tennessee; D.B.A., University of Tennessee; C.P.A., C.M.A., C.I.S.A. Associate Professor of Accounting, University of Tennessee.

[1] In a computer context, the term *access* means an individual's ability to get at the resources of a computer, including physical devices and data. Accessing data may involve reading, modifying, or erasing data items. Unauthorized access is access through which an unauthorized individual reads, modifies, or erases data for an impermissible purpose. *See* Note, *Hacking—The Unauthorised Access of Computer Systems; The Legal Implications*, 52 MOD. L. REV. 236, 237 (1989) [hereinafter Note, *Hacking—The Unauthorised Access*] ("Computer hacking is the accessing of computer-stored information without the permission of the owner of the computer system or the information.").

When computers were first invented, the term *hacker* was an appellation of honor, not a derogation. Programmers in academic research labs with access to early computers (in the late 1950s and the 1960s) took pride in improving the function and performance of the machines. Their philosophy embraced sharing and decentralization of computer knowledge, openness of discussion, and esteem for "innovation, style, and technical virtuosity." *See* S. LEVY, HACKERS: HEROES OF THE COMPUTER REVOLUTION 10 (1984). The skilled programmers, known as hackers, had an irresistible urge to understand the workings of others' programs and to use that understanding to improve those programs to the benefit of all machine users. To facilitate program improvement, hackers made all programs accessible to all users, who then "could go through the programs of the master hackers, looking for ideas, admiring the code. The idea was that computer programs belonged not to individuals, but to the world of users." *Id.* at 115. This ethos facilitated program improvements that were a great impetus to the development of better computer systems, but it was no match for the sense of property rights held by increasing numbers of users who valued the result of the computer's work and wanted to keep it and the programs that were generated private. Over time, *hacker* came to mean any individual who, mostly for the challenge of it, sought to access computer systems whether or not they were author-systems, many people were tolerant of the perpetrators' ingenuity because the results of the unauthorized access were benign.[2] Public reaction changed, however, when unauthorized access led to lost or scrambled files[3] and necessitated system downtime in order to cleanse

ized to do so. *See* Note, *Computer Crime and the Computer Fraud and Abuse Act of 1986*, 10 COMPUTER/L.J. 71, 73 n.11 (1990) [hereinafter Note, *Abuse Act*].

[2] *See* Reid, *Reflections on Some Recent Widespread Computer Break-Ins*, 30 COMM. OF THE ACM 103, 103-05 (1987).

Other reasons for ambivalence include: the necessity for special expertise in order to understand the technology of the crime; preparation of a case against a suspect can be time consuming and tedious; the "criminals" seem more clever than dangerous; and finally, large banks and businesses, rather than individuals, are the usual victims. Note, *Computer Viruses and the Law*, 93 DICK. L. REV. 625, 630 (1989) [hereinafter Note, *Computer Viruses*] (citing Gemignani, *What is Computer Crime, and Why Should We Care?*, 10 U. ARK. LITTLE ROCK L.J. 55, 56 (1987-88)); *see* Volgyes, *The Investigation, Prosecution, and Prevention of Computer Crime: A State-of-the-Art Review*, 2 COMPUTER/L.J. 385, 394-402 (1980) (discussing federal statutes regarding computer crime); Note, *Computer Crime Statutes: Are They Bridging the Gap Between Law and Technology*, 11 CRIM. JUST. J. 203, 206 (1988) [hereinafter Note, *Bridging the Gap*] (Most computer crimes are hard to detect; consequently, they go undetected and unpunished.).

Sometimes, these "criminals" are not prosecuted because no harm is done or the intruder is not detected. The fervor with which one prosecutes depends upon what the hacker does upon entry into the system.

> Once the hacker has penetrated the computer system he may do one of several things. He may just read or copy the information, which may be highly confidential; he may erase or change some or all of the information or he may simply add something, such as a message boasting of his feat. The legal implications depend upon which of these acts it is that the hacker performs. . . . The worrying point of this is that, although people such as these intend no harm, they demonstrate the weak security aspects of computer systems. If they can get in, then so can others who will have less agreeable motives.

Note, *Hacking—The Unauthorised Access*, *supra* note 1, at 237; *see also* Note, *Bridging the Gap*, *supra*, at 203 ("'Most non-violent crimes and even violent crimes such as homicide can be committed through or facilitated by computers.'" (quoting S. NYCUM & D. PARKER, PROSECUTORIAL EXPERIENCE WITH STATE COMPUTER CRIME LAWS 34 (1986))).

[3] These lost or scrambled files are sometimes the result of computer viruses.

> Computer viruses are computer instructions or small hidden programs that are inserted into a standard computer program or into a computer's operating system. These instructions may replicate many times during a single program execution, infect every program on a computer disk and be passed on secretly to other computers through modems, floppy discs, or network connections.
>
> A programmer creates a virus by writing a computer code which can attach itself to other programs. Once attached, this code may alter the operations of a program or destroy data kept on a computer disk. A virus can "infect" a computer system as a result of programming or by users running an already infected computer program on the system. Unsuspecting users running virus-infected programs allow the virus to establish itself in a computer system. Once established, the virus can access and modify any file the user is authorized to access. Similar to a biological virus, a computer virus spreads rapidly from a single point of infection. Multiplying in geometrical progression as it works its way through a com-

or reconstruct the systems.[4] When unauthorized access resulted in damage,[5] people began to look at computer systems as entities worthy

> puter system or network, the computer virus may contaminate all files within a computer system.
>
> A computer virus basically carries a genetic code in machine language. The virus may be benign or malicious. A malicious virus can cripple a network with dead-end tasks, erase files, create false information, and in some cases, destroy equipment.

Note, *Computer Viruses*, *supra* note 2, at 627 (footnotes omitted).

Other forms of a computer crippling code are logic bombs, time bombs and worms. A logic bomb is program code embedded in other code that, when triggered, is intended to exhibit destructive behavior. A time bomb is code that unleashes its destructive behavior at a preprogrammed time and date. A worm is code that replicates itself across computer systems. *Id.* at 628. For additional information on logic bombs and worms, see Gemignani, *supra* note 2, at 64 nn.38 & 39.

A more technical definition of a virus is as follows:

> [A] virus program is a program that has the following attributes: (1) It must be capable of modifying software not belonging to the virus by attaching its program structure to the other program. (2) It must be capable of executing this modification on a number of programs. (3) It must have the capability of recognizing the modification on other programs. (4) It must have the ability to prevent further modification of the same program upon recognition of a previous modification. (5) Modified software produced by the virus must have attributes (1) through (4). A program lacking any one of these characteristics is not technically considered a virus.

Note, *Computer Viruses: Is There a Legal "Antibiotic?"*, 16 RUTGERS COMPUTER & TECH. L.J. 253, 255 n.12 (1990) [hereinafter Note, *Legal Antibiotic*]; *see* BloomBecker, *Computer Crime Update: The View as We Exit 1984*, 7 W. NEW ENG. L. REV. 627 (1985).

[4] *See generally* Mace, *Virus Outbreaks Spur Congress to Combat Threat*, INFOWORLD, May 22, 1989, at 34, col. 5. The damages due to intruders have prompted the proposal of federal legislation to create "criminal penalties for knowingly inserting viruses that could cause loss, expense, or risk to health or welfare." *Id. See generally* Gemignani, *supra* note 2, at 55; Tunick, *Computer Law: An Overview*, 13 LOY. L.A.L. REV. 315, 326 (1980) ("Experts believe that computer crime is almost impossible to detect and that it costs the public at least $10 billion annually."); Note, *Who is Calling Your Computer Next? Hacker!*, 8 CRIM. JUST. J. 89, 89 (1985) [hereinafter Note, *Hacker!*]; Note, *Legal Antibiotic, supra* note 3, at 253 ("Between January and September of 1988 an estimated 250,000 U.S. computer users were affected by programs that could have potentially destroyed all valuable data within their computer systems.").

[5] Note, *Bridging the Gap, supra* note 2, at 206 ("Computer crime yields extraordinarily higher profits per incident than traditional fraud and theft. Estimates of the average proceeds have ranged from $10,517 to $450,000." (footnotes omitted)).

There are five categories of common computer crime: financial crimes, property crimes, information crimes, theft of services, and vandalism. In addition, there are five phases of computer operation during which a criminal can intervene in the process: input, programming, processing in the central processing unit, output and communication of data. Tunick, *supra* note 4, at 326, 328. *But see* Note, *Computer Abuse: The Emerging Crime and the Need for Legislation*, 12 FORDHAM URB. L.J. 73, 74-75 (1984) [hereinafter Note, *Computer Abuse*] ("Computer crime falls into four categories: (1) theft of money, financial instruments, property, services, or valuable data; (2) unauthorized access to computer time; (3) illegal use of computer programs; and (4) unauthorized acquisition of stored data." (footnotes omitted)).

of legal protection. As a result, state[6] and federal[7] computer crime[8] statutes have been enacted in the last five years,[9] and additional bills

[6] *See, e.g.*, CAL. PENAL CODE § 502 (West 1990); CONN. GEN. STAT. § 53a-251 (1989); FLA. STAT. ANN. § 815.01-07 (West Supp. 1990); TENN. CODE ANN. § 39-14-602 (Supp. 1990); TEXAS PENAL CODE ANN. § 33.02 (Vernon Supp. 1991); WIS. STAT. ANN. § 943.70 (1990).

For articles discussing state computer crime statutes, see BloomBecker, *supra* note 3, at 627; Branscomb, *Rogue Computer Programs and Computer Rogues: Tailoring the Punishment to Fit the Crime*, 16 RUTGERS COMPUTER & TECH. L.J. 1, 30-37 (1990); Gemignani, *Computer Crime: The Law in '80*, 13 IND. L. REV. 681, 710-15 (1980); Lederman, *Criminal Liability for Breach of Confidential Commercial Information*, 38 EMORY L.J. 921 (1989); Comment, *Computer Crime Deterrence*, 13 AM. J. CRIM. L. 391, 399-404 (1986); Note, *Bridging the Gap, supra* note 2, at 209-213, 220-23; Note, *Hacker!, supra* note 4, at 102-07; Note, *Abuse Act, supra* note 1, at 75-76; Note, *Computer Viruses, supra* note 2, at 641 (containing a list of relevant state statutes for forty-eight states); Note, *Computer Abuse, supra* note 5, at 89-94; Note, *An Overview of Recent Changes in California Computer Crime Laws: The Criminalization of Computer Contamination and Strengthened Penalty Provisions*, 6 SANTA CLARA COMPUTER & HIGH TECH. L.J. 135-42 (1990) (discussing significant changes in and additions to current California law dealing with computer crime and new antiviral legislation); *see also* Branscomb, *supra* at 37-44 (discussing state legislation pending in the Spring of 1989). *See generally* Nycum, *The Criminal Law Aspects of Computer Abuse: Part I: State Penal Laws*, 5 RUTGERS J. COMPUTERS & L. 271, 276-95 (1976).

For examples of cases litigated under the California statute, see People v. Lowery, 200 Cal. App. 3d 1207, 246 Cal. Rptr. 443 (1988); Mahru v. Superior Court, 191 Cal. App. 3d 545, 237 Cal. Rptr. 298 (1987); People v. Gopal, 171 Cal. App. 3d 524, 217 Cal. Rptr. 487 (1985).

[7] *See, e.g.*, Computer Security Act of 1987, Pub. L. No. 100-235, 101 Stat. 1725; Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848; The Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213. For law review articles discussing various federal computer crime statutes, see Branscomb, *supra* note 6, at 44-48; Lederman, *supra* note 6, at 931-32, 978-93; Comment, *supra* note 6, at 392-99; Note, *Bridging the Gap, supra* note 2, at 213-15, 217-20; Note, *Hacker!, supra* note 4, at 99-102; Note, *Abuse Act, supra* note 1, at 76-84; Note, *Computer Viruses, supra* note 2, at 636-38; Note, *Computer Abuse, supra* note 5, at 77-84; Note, *The Electronic Communications Privacy Act of 1986: The Impact on Software Communications Technologies*, 2 SOFTWARE L.J. 243 (1988).

[8] The delay in bringing about legislation may be due to the lack of agreement as to a definition of "computer crime." The following are samples of the various definitions employed. A. BEQUAI, COMPUTER CRIME 4 (1978) (A computer crime is "the use of a computer to perpetuate acts of deceit, concealment and guile that have as their objective the obtaining of property, money, services, and political and business advantages."); Taber, *A Survey of Computer Crime Studies*, 2 COMPUTER/L.J. 275, 298 (1980) (A genuine computer crime is "a crime that, in fact, occurred and in which a computer was directly and significantly instrumental.").

[9] Although computers have been used widely by society for a number of years, only recently has legislation been enacted. This is because some legislators have relied on the courts to fashion existing criminal laws to combat computer abuse. For examples of cases which have tried to construe existing law to extend to computer cases, see Gemignani, *supra* note 2, at 55-67. *See generally* Comment, *supra* note 6, at 394-95 (addressing specific examples of computer crimes which courts have been willing to classify as within federal criminal statutes). *But see* Taber, *On Computer Crime (Senate Bill S. 240)*, 1 COMPUTER/

were introduced in the 101st Congress.[10] The intent of these laws is to deter individuals from unauthorized access to the protected systems and to create penalties for such behavior.[11] Collectively, these laws treat computer systems as property worthy of protection against trespass and conversion.

Given the pervasiveness of computer systems and American society's dependence on them, the increased attention to unauthorized computer access is warranted. Focusing solely on the perpetrators of computer fraud, however, is unlikely to prevent access by unauthorized individuals or provide compensation for injured parties.[12] For example, perpetrators from abroad might not be within the reach of state and federal laws.[13] Skilled individuals will always be able to penetrate computer systems, and a single individual or a small group of individuals would likely be unable to compensate injured parties, even if they were within the jurisdictional purview of the statute.[14]

Although individual intruders may attack computer systems at random,[15] the more dangerous computer criminals are likely to be in-

L.J. 517, 518 (1979) ("[T]here is no such thing as a 'computer' crime, and therefore no need for special legislation addressing this 'problem.' ").

Likewise, some commentators have advanced the theory of extending the constitutional right of privacy, the common law right of privacy, and the right of privacy by statute to prevent computer abuse. Tunick, *supra* note 4, at 332-38.

[10] The two bills, H.R. 55, Virus Eradication Act, and H.R. 287, Computer Protection Act, were both intended to tighten protection of computer systems. While there is no unanimity about the need for computer crime statutes, the U.S. Government Accounting Office has charged that existing law is inadequate. *See* U.S. GOVERNMENT GENERAL ACCOUNTING OFFICE, PUB. NO. GAO/IMTEC-89-57, COMPUTER SECURITY: VIRUS HIGHLIGHTS NEED FOR IMPROVED INTERNET SECURITY (1989). One person has been charged under the 1986 Computer Fraud and Abuse Act for releasing a program that interfered with the operation of thousands of computers. *See* Wilke, *Student Indicted on Charge Linked to Computer Virus*, Wall St. J., July 27, 1989, at B7, col. 5.

For a summary of bills which Congress has considered, see Branscomb, *supra* note 6, at 48-49; Taber, *supra* note 9, at 518; Note, *Computer Abuse*, *supra* note 5, at 84-89.

[11] According to one commentator, "the focus of legislation should be on the nature of the asset subject to loss, rather than on the technology which is rapidly subject to obsolescence and requires repeated amendment." Note, *Bridging the Gap*, *supra* note 2, at 208.

[12] Samuelson, *Can Hackers Be Sued for Damages Caused by Computer Viruses?*, 32 COMM. OF THE ACM 666, 667 (1989).

[13] See Stoll, *Stalking the Wily Hacker*, 31 COMM. OF THE ACM 484, 489-90 (1988), for an account of the lengthy tracing of a German hacker's intrusion into American computer networks.

[14] See Spafford, *Crisis and Aftermath*, 32 COMM. OF THE ACM 678, 678-87 (1989), for an account of the chaos on Internet, an American computer network, caused by a single intruder.

[15] *See generally* Branscomb, *supra* note 6, at 6-30 (discussing several incidents involving rogue behavior in computer networks and the motivation behind these events).

siders who have some legitimate access to the system.[16] Ironically, organizations have been reluctant to prosecute insiders for fear of embarrassing publicity over the vulnerabilities of organizational computer systems.[17] Thus, society should not assume that laws addressing unauthorized use of computer systems will be sufficient protection for users.

In addition to legislating sanctions for perpetrators of computer break-ins, it is also appropriate to examine the responsibilities of people and entities providing and managing computer systems. According to one expert, Clifford Stoll, poor systems management contributed significantly to a recent trespass into military networks.[18] Stoll noted that after ten months of tracking the intruder, who attacked about 450 computers and successfully entered more than thirty of them, "[m]ost of these break-ins were possible because the intruder exploited common blunders [made] by vendors, users, and system managers."[19] He also noted, "[t]he security weaknesses of both systems and networks, particularly the needless vulnerability due to sloppy systems management and administration, result in a surprising success rate for unsophisticated attacks."[20]

Others have noted that lax implementation of security features and ineffective operating procedures make unauthorized access to computer systems simple.[21] Usually the damage is only to the system itself in the form of lost or destroyed data. Sometimes, however, personal injury may result. For example, Stoll stated that the same intruder who entered the military networks also accessed a computer which controlled the "real-time" administration of medical treatment. Had the intruder not been detected, a patient may have been severely injured.[22]

In a more widely publicized incident, a college student infected Internet, a network of computers for scientific research, with a pro-

[16] For examples of insiders who have caused computer abuse, see Tunick, *supra* note 4, at 328-30.

[17] *The Real Target*, Computerworld, Feb. 27, 1989, at 20, col. 1.

[18] Stoll, *supra* note 13, at 484.

[19] *Id.*

[20] *Id.* at 492.

[21] T. EISENBERG, D. GRIES, J. HARTMANIS, D. HOLCOMB, M. LYNN & T. SANTORO, THE COMPUTER WORM: A REPORT TO THE PROVOST OF CORNELL UNIVERSITY ON AN INVESTIGATION CONDUCTED BY THE COMMISSION OF PRELIMINARY ENQUIRY (Feb. 6, 1989) [hereinafter CORNELL UNIVERSITY]; Denning, *The Science of Computing: Computer Viruses*, 76 AM. SCIENTIST 236, 238 (1988).

[22] Stoll, *supra* note 13, at 489.

gram that reproduced itself on thousands of computers.[23] The result was a disruption of normal activities and network connectivity for over a week.[24] In another incident, an ex-employee of an insurance and brokerage firm was convicted of a felony for planting a computer time bomb in his former employer's computer system that was intended to erase payroll data once a month.[25] Clearly, there exists a growing number of incidents in which third parties are placed at risk due to unauthorized access to and misuse of organizational computer systems.

Even though it is impossible to maintain perfectly secure systems,[26] managers have a duty to provide reasonably secure systems by exercising care in the implementation and operation of their systems.[27] Part I of this article addresses the scope of potential negligence liability for the providers of computer services who fail to exercise reasonable care in securing and protecting their computer systems from unauthorized access.[28] Part II of the article describes steps computer

[23] For another account of this incident, see Note, *Computer Viruses*, *supra* note 2, at 625-26.

[24] *See generally* CORNELL UNIVERSITY, *supra* note 21; Rochlis & Eichin, *With Microscope and Tweezers: The Worm from MIT's Perspective*, 32 COMM. OF THE ACM 689 (1989); Spafford, *supra* note 14, at 678; *How Computer Science Was Caught Off Guard by One Young Hacker*, Wall St. J., Nov. 7, 1988, at A1, col. 1.

[25] Savage, *Computer Time Bomb Defused; Felon Nailed*, Computerworld, Sept. 26, 1988, at 2, col. 4.

[26] Perfectly secure systems would keep out authorized users too and hence would be of no use to their owners.

[27] For tips on devising and implementing an effective computer system, see Comment, *supra* note 6, at 404-15. *But see* Note, *Legal Antibiotic*, *supra* note 3, at 254 ("Increased security measures are only a partial solution because they serve to create a more inviting challenge to the person compelled to demonstrate his computer programming skill.").

[28] *See infra* notes 30-106 and accompanying text.

When an unknown and unauthorized "hacker" accesses personal data held by a private enterprise, the enterprise itself is the victim's only source of recovery. As one author noted:

> 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, however, it is first necessary to determine what general standards of care are expected from

managers might take to satisfy a duty of reasonable care to safeguard the systems they manage.[29]

I. Potential Liability for Negligence

Individuals who gain unauthorized access to computer systems may be criminally[30] and civilly liable for their actions. It is also true, however, that in each of the cases noted above there were steps the computer systems manager could have taken to significantly lessen the ease with which the intruder gained access to the affected computer system. In the case involving the Lawrence Berkeley Laboratory (LBL) and medical treatment break-ins, the systems manager did not enforce password expiration, require non-obvious passwords, delete expired accounts, or eliminate shared accounts. Taken together, these precautions would have reduced the risk of unauthorized access.[31] In the Internet incident, the intruder exploited documented flaws in ven-

> businesses which hold confidential data. If the injured party can prove the enterprise failed to exercise the standard of care required, he may recover. The problem is that there are no generally accepted standards with which to ascertain the degree of security required of any business. Thus, practitioners must persuasively argue that the business failed to meet even the most basic level of protection.

Agranoff, *Curb on Technology: Liability for Failure to Protect Computerized Data Against Unauthorized Access*, 5 Santa Clara Computer & High Tech. L.J. 263, 268 (1989) (footnotes omitted); *see also* Ware, *Computer Security Standards for Government and Industry: Where Will They Come From?*, Computer Security J. 71 (1983).

[29] *See infra* notes 107-44 and accompanying text.

[30] Betts, *Senate Takes Tentative Look at Virus Legislation*, Computerworld, May 22, 1989, at 8, col. 3. Existing federal laws generally require proof of criminal intent and damage, making prosecution of some intruders, for example, the perpetrator of the Internet worm, difficult. New legislation has been proposed to fill this gap. *See supra* note 10 and accompanying text.

[31] Stoll, *supra* note 13, at 490. Other possible security measures include:

> (1) Even if there is a general password to access a . . . file, each authorized individual should also have a password that is unique and not known to other individuals; (2) The password should not be a proper name, common . . . term [associated with the business], or other easily-guessed item. It should be changed regularly. These mandates should be enforced by software; (3) After a small number of incorrect passwords, the line into the computer should be disconnected and security personnel promptly notified; (4) Encryption should be considered if extremely sensitive data is involved; (5) A contingency plan should be developed and tested in the event that phone lines into the computer are down for an extended period of time, ensuring that the computer can be updated "on site;" (6) Access control software should clearly define what users can access what data, under what conditions, and supported by a proper chain of authorized signatures; (7) Violation reports should be manageable and designed to produce adequate follow-up action; (8) Regular audits of computer security should be conducted by personnel trained in technical and administrative techniques, who are not employed by the data processing department.

Agranoff, *supra* note 28, at 271 n.20. In addition, one commentator urges education on dor-supplied software for which there were known remedies.[32] In the payroll case, the company took cursory but not thorough steps to deny access to the former employee.[33]

Since the actual wrongdoers in cases like these may not have the resources to compensate those injured by computer fraud, injured plaintiffs are likely to look for deeper pockets for their compensation. Managers with responsibility for an organization's computer systems may learn that their inexperience, lack of knowledge, or simple procrastination in protecting their systems will expose their organizations to civil liability for negligence in the operation of the systems.

A. *Analysis of Negligence Actions Against Managers*[34]

Many computer systems managers would be appalled to learn that the actions of individuals obtaining unauthorized access to their systems could expose their employers to liability for resulting damages. Nonetheless, although there are no recorded cases on point,[35] general principles of negligence[36] provide precedent for the imposition

computer abuse to bring computer crime under control. Note, *Abuse Act*, *supra* note 1, at 84-86.

[32] Spafford, *supra* note 14, at 678-84.

[33] Savage, *supra* note 25, at 2.

[34] This article focuses on the potential liabilities of information systems managers. For an analysis of similar issues surrounding electronic bulletin board managers, see Soma, Smith & Sprague, *Legal Analysis of Electronic Bulletin Board Activities*, 7 W. NEW ENG. L. REV. 571 (1985).

[35] A case, however, decided by the United States Court of Appeals for the Fifth Circuit is worth noting in this context. Thompson v. San Antonio Retail Merchants Association, 682 F.2d 509 (5th Cir. 1982) concerns a claim based on the Fair Credit Reporting Act (the "Act"), 15 U.S.C. § 1681 (1988). Section 1681o of the Act states that a consumer reporting agency is liable to consumers in the event of failure to`comply with the requirements of the Act. Among its requirements, the Act provides: "Whenever a consumer reporting agency prepares a consumer report it shall follow *reasonable procedures* to assure maximum possible accuracy of the information concerning the individual about whom the report relates." 15 U.S.C. § 1681e(b) (1988) (emphasis added).

In *Thompson*, the plaintiff argued that the San Antonio Retail Merchants Association (SARMA) had failed to implement reasonable computer practices, and, as a result, had provided erroneous credit reports to several organizations from which he attempted to obtain credit. *Thompson*, 682 F.2d at 511-12.

The trial court held that SARMA "failed to exercise reasonable care in programming its computer to automatically capture information into a file." *Id.* at 513.

Although the basis of liability in the case is a federal statute rather than a common law negligence claim, it is significant that the court recognized that misuse of computers, based on a reasonable-person standard, could be the basis of liability for the provider of computer services.

[36] *See generally* Comment, *"Computer Malpractice" and Other Legal Problems Posed by Computer "Vaporware"*, 33 VILL. L. REV. 835, 892 (1988) (advocating that "the judiciary should be more amenable to computer tort claims, and adopt computer malpractice as a viable cause of action").

of liability on systems managers.[37]

"[N]egligence is defined as 'the failure to exercise that degree of care that an ordinarily prudent person would exercise under the same or similar circumstances and when charged with like duty.' "[38] In order for the provider of computer services to be deemed legally negligent,[39] the injured party would have to prove the traditionally recognized elements of negligence: that the provider of computer services had a duty to the injured party to exercise reasonable care in the creation, installation, or operation of the computer system; that the systems manager breached that duty by failing to exercise the requisite care; that the breach of that duty was the proximate cause of the injury to the plaintiff; and that the plaintiff did in fact suffer physical injury, property damage or economic harm as a result of the breach.[40]

1. Duty of Reasonable Care

To hold a systems manager's employer liable for negligence, the plaintiff must first establish that the company, in the person of the systems manager, owed a duty to the plaintiff to exercise reasonable or ordinary care in providing computer services.[41] Reasonable care is

[37] *See* Fossett, *The Development of Negligence in Computer Law*, 14 N. KY. L. REV. 289, 293-95 (1987) (arguing that negligence on the part of a computer user is appropriately addressed by a claim in tort).

[38] Tharpe v. Brewer, 7 N.C. App. 432, 438, 172 S.E.2d 919, 924 (1970) (quoting Williamson v. Clay, 243 N.C. 337, 345, 90 S.E.2d 727, 733 (1956)).

[39] One commentator described negligence as follows:

> *Negligence*. Negligence occurs when an individual has failed to exercise prescribed duties or has failed to carry out those duties in a prudent manner. Negligence may arise because of either nonfeasance or malfeasance, and may be the result of an error of commission or omission on the part of [those] . . . defending a lawsuit.
>
> . . . .
>
> Courts will be looking at the question of negligence in order to decide whether it was of such a nature as to be considered "ordinary" or "gross." *Ordinary negligence* normally involves an act or a failure to act that resulted from simple carelessness or basic human error. At the other extreme, *gross negligence* involves what the court finds to be a reckless, willful, or wanton act or failure to act in view of the circumstances. . . . In computer fraud cases, the existence of *scienter*, or intent, on the part of the defendants may hinge on whether the negligence is adjudged to be ordinary or gross, the implication being that gross negligence translates to intent.

L. KRAUSS & A. MACGAHAN, COMPUTER FRAUD AND COUNTERMEASURES 337 (1979).

[40] W. KEETON, PROSSER AND KEETON ON THE LAW OF TORTS § 30, at 164-65 (1984).

One commentator has noted that "the modern computer is not, for the most part in its current use today, a physically dangerous machine." Fossett, *supra* note 37, at 291. Consequently, computers do not usually cause physical injury or property damage. *Id.*

[41] "[E]very case is governed by the rule of general application that all persons are

generally defined as that degree of care that a similarly situated reasonable person would exercise.[42] The duty of reasonable care has limits: the injured party must typically show that the defendant owed both a duty to the plaintiff and a duty to act or refrain from acting to avoid foreseeable harm. The concept of duty is a limitation on the scope of liability.[43] Thus, duty imposes an obligation only towards those who would be foreseeably endangered and only with respect to those risks or hazards that are reasonably foreseeable. The manager of a computer system would have a duty to use reasonable care to secure the system[44] when it is reasonably foreseeable that failure to secure it would result in injury to others. While "others" encompasses a potentially unlimited group, there are limits on how far liability would extend. A duty of care runs only to "foreseeable plaintiffs," any person or class of persons who could reasonably be expected to be injured by the systems manager's negligence. Although the manager's scope of duty is also limited to the kinds of injury that could reasonably be foreseen, the exact manner in which the injury is brought about need not be foreseeable.[45] The presence or absence of a systems manager's duty to protect a plaintiff will be a function of the facts of a particular

required to use ordinary care to prevent others from being injured as a result of their conduct." J'Aire Corp. v. Gregory, 24 Cal. 3d 799, 806, 598 P.2d 60, 64, 157 Cal. Rptr. 407, 411 (1979) (quoting Weirum v. RKO Gen., Inc., 15 Cal. 3d 40, 46, 539 P.2d 36, 39, 123 Cal. Rptr. 468, 471 (1975)).

[42] "[N]egligence 'consists in a want of that reasonable care which would be exercised by a person of ordinary prudence *under all the existing circumstances* . . . .' " Gowdy v. United States, 271 F. Supp. 733, 738 (W.D. Mich. 1967) (quoting Detroit & M.R.R. v. Van Steinburg, 17 Mich. 99, 118-19 (1868)), *rev'd* 412 F.2d 525, *cert. denied*, 396 U.S. 960 (1969).

[43] 3 F. HARPER, F. JAMES & O. GRAY, THE LAW OF TORTS § 18.2 (1986).

[44] There are various methods to protect a computer system, for example:

> Numerous security measures have been suggested for safeguarding the computer system from criminal attack. Some experts suggest that the system itself be kept under guard and be isolated from the other divisions of a firm. It is suggested, further, that the programmer not operate the computer. In addition, experts note that no employee should have access for too long a period of time to any one stage of the computer's operation. Access should be on a need-to-know basis only.
>
> However, a computer can be safeguarded but never made fully impregnable. The primary factor behind computerization has been the economic motive. Extreme security measures could easily nullify the economic feasibility of a computer system. . . . There is a need for deterrence, which only law enforcement and prosecution can provide. However, at present, our investigatory and prosecutorial machinery has been slow to adapt to this new form of crime.

A. BEQUAI, WHITE-COLLAR CRIME: A 20TH-CENTURY CRISIS 109 (1978) (endnotes omitted).

[45] *See, e.g.*, R. KEETON, LEGAL CAUSE IN THE LAW OF TORTS 49-61 (1963).

case.[46]

2. Breach of Duty

Next, a potential plaintiff must show that a manager breached his or her duty of reasonable care. A systems manager might be found to have breached a duty of reasonable care for a number of reasons, such as the failure to recognize defects in a system, the failure to correct defects, or the failure to warn of defects.[47] Because of the number of ways a computer can malfunction, proving negligence will be difficult.[48] Breach of duty might also arise from failure to train and supervise employees,[49] or the failure to use reasonable means to secure the system from unauthorized and unintended use.

3. Proximate Cause of Injury

The third element of a negligence claim is proof that the defendant's act, or failure to act, was the proximate cause of the plaintiff's injury.[50] Stated generally, satisfying the element of proximate cause requires first, that the defendant's action be an actual cause, and second, that the consequences of that act were foreseeable.[51] Finally, the plaintiff will need to prove that he or she was a foreseeable victim.[52] There can be more than one proximate cause of an injury.[53] For example, in the case of the Internet intruder,[54] the cause in fact of the injury was the illegal or unauthorized act of accessing the computers

[46] "The circumstances of each case supply the features from which breaches of duty and negligence arise." Gowdy v. United States, 271 F. Supp. 733, 738 (W.D. Mich. 1967).

[47] "There can be little doubt that the use of computer resources is changing the practice standards [of design engineers]. It is not difficult today to anticipate the misuse of computerized resources as negligence." Lurie & Weiss, *Computer Assisted Mistakes: Changing Standards of Professional Liability*, 2 SOFTWARE L.J. 283, 285 (1988).

[48] Note, *Easing Plaintiffs' Burden of Proving Negligence for Computer Malfunction*, 69 IOWA L. REV. 241 (1983) (proposing a liberal use of the "res ipsa loquitur" doctrine in computer injury claims).

[49] 3 F. HARPER, F. JAMES & O. GRAY, *supra* note 43, at § 18.7.

[50] W. KEETON, *supra* note 40, § 30, at 165. For a complete overview of the causation issue in the common law, see Kratzke, *The Convergence of the Discretionary Function Exception to the Federal Tort Claims Act With Limitations of Liability in Common Law Negligence*, 60 ST. JOHN'S L. REV. 221, 228-32 (1986).

[51] The concept of "proximate cause" is subject to varied definitions. Black's Law Dictionary states that "[a]n injury or damage is proximately caused by an act, or a failure to act, whenever it appears from the evidence in the case, that the act or omission played a substantial part in bringing about or actually causing the injury or damage; and that the injury or damage was either a direct result or a reasonably probable consequence of the act or omission." BLACK'S LAW DICTIONARY 1225 (6th ed. 1990).

[52] Palsgraf v. Long Island R.R., 248 N.Y. 339, 162 N.E. 99 (1928).

[53] W. KEETON, *supra* note 40, § 44, at 301-02.

[54] *See supra* note 23 and accompanying text.

on the Internet network, but the insufficient security system was also a cause. Even where the intervening act is illegal and unauthorized, a provider of computer services may not be relieved from liability for negligence due to failure to restrict access to a system.[55] If it was reasonably foreseeable that the system might be sabotaged, the manager will be required to use reasonable means to protect against intrusion. While the manager cannot be required to impose absolute security, he or she should be charged with implementing reasonable access control.

Reasonableness can be determined by several factors.[56] First, the amount of caution required increases with the likelihood of injury.[57] Second, as the severity of possible harm increases, the duty to protect against the harm likewise increases.[58] Thus, greater and more comprehensive measures would be expected for a system with critical or sensitive data. Third, the cost of avoiding foreseeable harm is also relevant.[59] The cost of protection will be balanced against the degree of risk and the seriousness of the possible resulting harm.[60] Where the cost of protection in time or money is low, there may be a duty to protect against even remote risks.[61] The manager will not be negligent, however, where the cost of restricting access is significantly out of proportion to the risks.[62]

As previously noted, a negligent or willful act, such as introducing a virus into a computer, could be the cause in fact of the resulting damage, such as altered or destroyed files or a system shutdown due to overload. The individual who introduces the virus may face criminal liability under the Computer Fraud and Abuse Act,[63] as well as civil

[55] *See infra* note 64 and accompanying text.

[56] Reasonableness is often a function of cost. For example, one commentator noted:

> Computer security generally is concerned with the implementation of controls to meet exposures. Normally, however, only cost effective controls are considered. . . . Such a process is usually termed a risk assessment or risk analysis. 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.

Agranoff, *supra* note 28, at 282-83 (footnotes omitted).

[57] 3 F. HARPER, F. JAMES & O. GRAY, *supra* note 43, § 16.9, at 469.

[58] *Id.* at 471.

[59] *Id.* at 477; *see also* Agranoff, *supra* note 28, at 276-308.

[60] 3 F. HARPER, F. JAMES & O. GRAY, *supra* note 43, § 57, at 477.

[61] *Id.*

[62] *Id.*

[63] *See, e.g.*, Alexander, *Morris Indicted in Internet Affair*, Computerworld, July 31, 1989, at 8, col. 1. Robert T. Morris, who allegedly planted a worm which shut down

penalties. But the provider of computer services may also be liable, unless the acts of the first individual are deemed to be superseding, which would cut off the provider's liability.[64] The provider's liability will depend upon the scope of the original foreseeable risk that the manager created through lax security practices. "If the intervening cause is one which in ordinary human experience is reasonably to be anticipated, or one which the defendant has reason to anticipate under the particular circumstances, the defendant may be negligent, among other reasons, because of failing to guard against it."[65] Because the courts generally agree that only foreseeable causes of harm will not supersede the defendant manager's liability,[66] the provider of computer services will be liable only if the intervening cause was foreseeable.[67] Once it is determined that the systems manager has a duty to anticipate the intervening misconduct and guard against it, this misconduct cannot supersede the liability of a provider of computer services.[68]

The same result would follow even if the hacker's actions constituted criminal conduct. Normally, one may proceed upon the assumption that others will obey the law.[69] However, where past experience indicates that criminal conduct should reasonably be anticipated, and especially when the potential injury is serious, the systems manager is presumably still liable to those harmed by the failure to safeguard the system.[70] Dean William Prosser cites the following as

thousands of computers on the nationwide Internet network, is the first person to face federal prosecution under the Computer Fraud and Abuse Act of 1986. In January, 1990, Robert Morris was found "guilty of illegally running a worm program on thousands of computers scattered across the country." Alexander, *Morris Verdict Stirs Debate,* Computerworld, Jan. 29, 1990, at 1, col. 3.

[64]
> The act of a third person in committing an intentional tort or crime is a superseding cause of harm to another resulting therefrom, although the 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).

[65] W. KEETON, *supra* note 40, § 44, at 303 (footnote omitted).

[66] *Id.* at 303-04.

[67] *Id.* at 302.

[68] *Id.* at 305.

[69] W. KEETON, *supra* note 40, § 33, at 198-99; *see, e.g.*, Watson v. Kentucky & I.B.R.R. Co., 137 Ky. 619, 126 S.W. 146 (1910) (criminal act of another was the intervening act that broke the chain of causation).

[70] The criminal conduct of others does not break the chain of causation where there have been prior similar criminal incidents. *See* 3 F. HARPER, F. JAMES & O. GRAY, *supra* note 43, § 16.12, at 495-96.

common examples of this concept: "if valuable property is left unguarded and exposed to the public view, it may be anticipated that it will be stolen; if the key is left in the lock of a jewelry store over a holiday, it is not at all unlikely that there will be a burglary."[71]

Similarly, if a computer system is left unprotected, it is likely that information in that system will be stolen, altered, or lost. With the risk of misconduct clearly foreseeable, the manager must use reasonable means to restrict access to the system.

4. Injury

The final element a plaintiff must prove in a negligence action is that he or she has suffered an injury.[72] This element raises an interesting issue in computer cases in that the injuries suffered are often purely economic.[73] While one can readily envision circumstances in which a security breach or a software malfunction could result in physical injury,[74] most of the injuries will be economic.[75] The exact form or manner of conceivable injuries is virtually unlimited.

Traditionally, English and American courts have denied negligence claims for purely economic losses.[76] This prohibition, sometimes called the per se prohibitory rule,[77] bars recovery for economic losses unaccompanied by physical injury or property damage.[78] The

[71] W. KEETON, *supra* note 40, § 33, at 203.

[72] *Id.* § 30, at 165.

[73] *See, e.g.*, Office Supply Co. v. Basic/Four Corp., 538 F. Supp. 776 (E.D. Wis. 1982) (California law does not allow recovery for economic loss in computer-related negligence claim.).

[74] See generally Massingale & Borthick, *Risk Allocation for Injury Due to Defective Medical Software*, 11 J. PROD. LIAB. 181 (1988), for a discussion of physical injury and death which resulted from software malfunction involving the use of computer-assisted radiation therapy. For a discussion of injuries involved in computer use in engineering, see Lurie & Weiss, *supra* note 47.

[75] *See generally* Reed, *Negligence and Computer Software*, 1987 J. BUS. L. 444.

[76] Note, *TORTS—DAMAGES—New Jersey Recognizes Negligence Action for Purely Economic Losses Unaccompanied by Physical Harm*—People Express Airlines, Inc. v. Consolidated Rail Corp., 100 N.J. 246, 495 A.2d 107 (1985), 17 SETON HALL L. REV. 719 (1987) [hereinafter Note, *New Jersey*]; *see also* Harvey, *Economic Losses and Negligence*, 50 CANADIAN B. REV. 580, 581-82 (1972); James, *Limitations on Liability for Economic Loss Caused by Negligence: A Pragmatic Appraisal*, 25 VAND. L. REV. 43, 45-46 (1972).

[77] Note, *Purely Economic Loss: A Standard for Recovery*, 73 IOWA L. REV. 1181, 1188 (1988) [hereinafter Note, *Purely Economic Loss*] (reviewing the history of the per se rule); Note, *New Jersey, supra* note 76, at 719; *see also* People Express Airlines v. Consolidated Rail Corp., 100 N.J. 246, 251, 495 A.2d 107, 109 (1985).

[78] Note, *Purely Economic Loss, supra* note 77, at 1182 n.3 (listing the leading cases barring recovery for purely economic loss); *see also People Express Airlines*, 100 N.J. at 251, 495 A.2d at 109; Note, *New Jersey, supra* note 76, at 719.

policy reasons for limiting or denying recovery for purely economic loss were based, in part, on the fear of exposing a defendant to unlimited liability, which might be too severe given his conduct.[79] However, there are numerous problems with this position, and in recent years courts have used several alternative lines of reasoning to limit the scope of liability while at the same time creating numerous exceptions to the per se prohibitory rule.[80]

Some of the early cases that allowed recovery for purely economic harm absent physical injury limited the scope of liability of the defendant by requiring a special relationship between the tortfeasor and a foreseeable plaintiff.[81] Eventually, some courts began to focus on foreseeability rather than physical damages as a means of limiting liability, even when a special relationship did not exist.[82]

The physical harm rule was traditionally premised on policy concerns of preventing mass litigation, fraudulent claims, and liability disproportionate to the defendant's fault.[83] The physical harm rule, however, was intended to limit, not deny, recovery for economic

[79] Dente, *Negligence Liability to All Foreseeable Parties for Pure Economic Harm: The Final Assault Upon the Citadel*, 21 WAKE FOREST L. REV. 587, 589 (1987); Rabin, *Tort Recovery for Negligently Inflicted Economic Loss: A Reassessment*, 37 STAN. L. REV. 1513, 1534 (1985); Note, *Recent Cases*, 88 HARV. L. REV. 444, 448 (1974).

[80] *See* Sharon Steel Corp. v. Lakeshore Inc., 753 F.2d 851, 856 (10th Cir. 1985) (economic losses allowed under New Mexico law); Babson Bros. Co. v. Tipstar Corp., 446 N.E.2d 11, 15 (Ind. Ct. App. 1983) (economic loss allowed if proximately caused); Groppel Co. v. United States Gypsum Co., 616 S.W.2d 49, 58 (Mo. Ct. App. 1981) (economic loss allowed without accompanying physical damage). *See generally* James, *Economic Loss: The Floodgates*, 1987 DENNING L.J. 97 (discussing three rationales which courts have used: reasonable foresight, economic loss recovery only where accompanied by injury to person or property, and the loss/reliance mechanism).

[81] *See, e.g.*, Lucas v. Hamm, 56 Cal. 2d 583, 364 P.2d 685, 15 Cal. Rptr. 821 (1961) (tort liability may be based on relationship between attorney who drafted will negligently and plaintiffs who lost inheritance as a result), *cert. denied*, 368 U.S. 987 (1962); Rozny v. Marnul, 43 Ill. 2d 54, 250 N.E.2d 656 (1969) (finding tort liability where error by land surveyor resulted in substantial costs to plaintiff purchaser of house despite the fact that survey was not contracted for by plaintiffs); Glanzer v. Shepard, 233 N.Y. 236, 135 N.E. 275 (1922) (tort liability may be based on relationship between public weighers of merchandise who erroneously certified weight of product and purchasers of product).

[82] J'Aire Corp. v. Gregory, 24 Cal. 3d 799, 804, 598 P.2d 60, 63, 157 Cal. Rptr. 407, 410 (1979) (finding tort liability on part of building contractor where renovations took excessive amount of time and cost plaintiff lessee lost revenues, because it was foreseeable that defendant's activity would affect plaintiff); H. Rosenblum, Inc. v. Adler, 93 N.J. 324, 352, 461 A.2d 138, 153 (1983) (liability established where stockholder suffered loss from independent auditor's inaccurate public statement).

[83] People Express Airlines v. Consolidated Rail Corp., 100 N.J. 246, 252, 495 A.2d 107, 110 (1985) (construing Kinsman Transit Co. v. City of Buffalo, 388 F.2d 821, 823 (2d Cir. 1968)); *see also* Note, *Purely Economic Loss*, *supra* note 77, at 1190-94.

loss.[84] In *People Express Airlines v. Consolidated Rail Corporation*,[85] the New Jersey Supreme Court cited several objectives to be furthered in allowing recovery for purely economic harm within certain parameters. These objectives included the need to compensate innocent victims for their injury, the need to discourage similar negligent behavior in the future, the need to foster safer products, a desire to vindicate reasonable conduct that shows regard for safety, and the need to shift costs of dangerous activities to those better able to sustain such costs.[86]

In an effort to balance these competing objectives, the New Jersey Supreme Court specifically rejected the per se prohibitory rule and allowed People Express Airlines to pursue its claim for purely economic loss when a railway accident caused a tank car containing flammable liquid to spill into a freight yard and ignite.[87] The spill, which presented a threat of explosion and other health hazards, forced the evacuation of the area within a one-mile radius of the accident site.[88] Although the fire was contained and an explosion never occurred, the accident forced the People Express Airlines' reservation office, located in the affected area, to interrupt its business operations for twelve hours, which resulted in substantial financial losses.[89] The New Jersey Supreme Court upheld the appellate court's decision, which found that recovery was not automatically barred by the absence of physical damages.[90] The New Jersey Supreme Court stressed that recovery for purely economic losses would be limited to plaintiffs, or classes of plaintiffs, whom the defendant knew or had reason to know would likely suffer damages due to the defendant's conduct.[91] The *People*

[84] *People Express Airlines*, 100 N.J. at 254, 495 A.2d at 111.

[85] 100 N.J. 246, 495 A.2d 107 (1985).

[86] *Id.* at 255, 495 A.2d at 111.

[87] *Id.* at 267-68, 495 A.2d at 118.

[88] *Id.* at 249, 495 A.2d at 108.

[89] *Id.* at 249-50, 495 A.2d at 108-09.

[90] *Id.* at 250, 495 A.2d at 109.

[91] The New Jersey Supreme Court stated:

> We conclude therefore that a defendant who has breached his duty of care to avoid the risk of economic injury to particularly foreseeable plaintiffs may be held liable for actual economic losses that are proximately caused by its breach of duty. In this context, those economic losses are recoverable as damages when they are the natural and probable consequence of a defendant's negligence in the sense that they are reasonably to be anticipated in view of defendant's capacity to have foreseen that the particular plaintiff or identifiable class of plaintiffs . . . is demonstrably within the risk created by defendant's negligence.

Id. at 267, 495 A.2d at 118.

Express decision illustrates that the courts can effectively limit the scope of liability for economic harm without requiring physical injury.

One difficulty in allowing recovery for property damage, but not for economic loss, is that the distinction between the two is unconvincing.[92] For example, if a car is negligently damaged, the owner complains about the cost of repair — an economic loss.[93] The requirement of physical injury to person or property before compensation for economic loss may lead to obviously unjust results:

> [T]he distinction between physical and economic loss brings us to the ridiculous point that if the same plaintiff suffers economic loss arising out of a physical injury and also similar economic loss (but not arising from physical injury) in consequence of the same wrongful act[,] he can recover under the one head but not under the other.[94]

In lieu of requiring physical damage as a means of limiting the defendant's scope of liability, many courts have required that the defendant's duty be limited by contract law. Where parties have voluntarily entered into a relationship having the features of a contract, the law enforces only those terms agreed to in the bargain. With respect to negligence in the provision of computer services, it may be that to impose duties that were never mutually assented to by the parties would be inherently wrong.[95]

[92] Edmeades, *The Citadel Stands: The Recovery of Economic Loss in American Products Liability*, 27 CASE W. RES. 647, 651 (1977); Fallon, *Physical Injury and Economic Loss — The Fine Line of Distinction Made Clearer*, 27 VILL. L. REV. 483, 484-85 (1981-82); James, *supra* note 80, at 103.

[93] James, *supra* note 80, at 103. Consider also the example given by Judge Kaufman in Kinsman Transit Co. v. City of Buffalo, 388 F.2d 821 (2d Cir. 1968):

> To anyone familiar with N. Y. traffic there can be no doubt that a foreseeable result of an accident in the Brooklyn Battery Tunnel during rush hour is that thousands of people will be delayed. A driver who negligently caused such an accident would certainly be held accountable to those physically injured in the crash. But we doubt that damages would be recoverable against the negligent driver in favor of truckers or contract carriers who suffered provable losses because of the delay or to the wage earner who was forced to "clock in" an hour late. And yet it was surely foreseeable that among the many who would be delayed would be truckers and wage earners.

Id. at 825 n.8.

[94] James, *supra* note 80, at 103-04; *see also* Spartan Steel & Alloys Ltd. v. Martin (Contractors) Ltd., [1973] Q.B. 27.

[95] In an analogous situation, a majority of the members of the Special Committee on Computers and the Law of the New York Bar Association indicated that in cases of claims against vendors of defective software, resulting in purely economic injuries, "traditional contract law should apply." Special Committee on Computers and the Law, *Tort Theories in Computer Litigation*, 38 REC. A. B. CITY N.Y. 426, 427 (1983). Dissenting

There is some argument that contract theories rather than negligence theories should control all computer cases resulting in economic loss.[96] However, this approach does not address the many incidents in which computer use or malfunction causes injury to third parties who were not parties to the initial bargain.[97] For example, suppose an unauthorized individual corrupts the files of a credit bureau which issues an erroneous credit report, causing a bank to deny credit to a business which then fails due to lack of credit. The damages are essentially economic, and there is no privity of contract between the business and the credit bureau.[98] However, to deny recovery in this instance for lack of privity of contract is fundamentally unfair. Arguably, it would be more appropriate to allow the injured party to seek recovery in tort and limit the scope of the credit bureau's liability under concepts of foreseeability and proximate cause.[99]

Although the road to tort recovery for purely economic loss has been long and circuitous in the American court system,[100] some recent decisions point toward recovery for economic harm based on reasonable foreseeability.[101] While the ability to collect for purely economic injury is uncertain, tort theories of recovery will continue to be asserted. The legal system must develop means to address the unique issues emerging as society rapidly grows more computer-dependent and the potential for serious economic harm to computer users increases. To avoid unjustified liability for the providers of computer services, careful assessments must be made as to the kinds of precautions a systems manager could reasonably take to safeguard computer

members of the committee were not willing to foreclose the possibility of tort liability in appropriate circumstances. *Id.* at 445.

[96] *See, e.g.*, Conley, *Tort Theories of Recovery Against Vendors of Defective Software*, 13 RUTGERS COMPUTER & TECH. L.J. 1 (1987); Fossett, *supra* note 37, at 292; Gemignani, *Product Liability and Software*, 8 RUTGERS J. COMPUTERS, TECH. & L. 173, 189-96 (1981); Nycum, *Liability for Malfunction of a Computer Program*, 7 RUTGERS J. COMPUTERS, TECH & L. 1, 9-15 (1979).

[97] Fossett, *supra* note 37, at 291-92 (arguing that this is why computer tort claims are on the rise).

[98] A credit reporting service that misidentified an individual as a bad credit risk has been found "negligent by failing to exercise reasonable care when programming its computer to capture and disseminate information correctly." *See* LaPlante, *Liability in the Information Age*, INFOWORLD, Aug. 18, 1986, at 37.

[99] *See supra* notes 50-71 and accompanying text.

[100] *See generally* Dente, *supra* note 79 (discussing the evolution of recovery for purely economic injury); Note, *Purely Economic Loss*, *supra* note 77 (regarding the historical and policy basis of the per se rule).

[101] *See, e.g.*, J'Aire Corp. v. Gregory, 24 Cal. 3d 799, 598 P.2d 60, 157 Cal. Rptr. 407 (1979); People Express Airlines v. Consolidated Rail Corp., 100 N.J. 246, 495 A.2d 107 (1985); H. Rosenblum, Inc. v. Adler, 93 N.J. 324, 461 A.2d 138 (1983).

resources. Actions constituting reasonable care on a systems manager's part must be defined.

B. *Statute of Limitations*

Even where all the elements of a negligence action are present, a claim for relief may be barred by a statute of limitations.[102]

In ordinary negligence actions, the statute begins to run once the negligent act or omission that caused the damage occurs.[103] However, when a hacker infiltrates a computer system with a "time bomb,"[104] this will present a different legal problem. Did the harmful act occur when the hacker first breached the computer's security, when the virus became active, or when the effect was first realized?

One author suggests the courts resolve this question by analogy to professional malpractice negligence.[105] The statute of limitations in many states does not begin to run in malpractice actions until the "time of discovery." However, to date, no court has adopted the concept of "computer malpractice."[106]

II. Defining the Duty of Care for Systems Managers

In the event of a suit charging a provider of computer services with negligence, one of the principal issues to be examined, assuming the existence of a duty,[107] will be whether the systems manager exercised reasonable care in safeguarding the computer resources at issue. This Section will define responsible managerial practices to which the court may look in determining whether a manager has in fact met the duty of reasonable care.

[102] "Statutes of the federal government and various states setting the maximum time periods during which certain actions can be brought or rights enforced. After the time period set out . . . has run, no legal action can be brought . . . ." BLACK'S LAW DICTIONARY 927 (6th ed. 1990).

[103] *See, e.g.*, H. Hirschfield Sons, Co. v. Colt Indus. Operating Corp., 107 Mich. App. 720, 309 N.W.2d 714 (1981) (Where truck scales were negligently installed, the statute ran from the date of the wrong, not when damage occurred.).

[104] *See supra* note 3 and accompanying text.

[105] Comment, *Computer Malpractice: Are Computer Manufacturers, Service Bureaus, and Programmers Really the Professionals They Claim to Be?*, 23 SANTA CLARA L. REV. 1065, 1089-91 (1983).

[106] Triangle Underwriters, Inc. v. Honeywell, Inc., 604 F.2d 737, 744 (2d Cir. 1979) (negligence action regarding computer installation barred by statute of limitations); *see also* Chatlos Sys. v. National Cash Register Corp., 479 F. Supp. 738, 740-41 n.1 (D.N.J. 1979) ("Simply because an activity is technically complex and important to the business community does not mean that greater potential liability must attach. . . . [T]he Court declines the invitation to create a new tort."), *aff'd*, 635 F.2d 1081 (3d Cir. 1980).

[107] *See supra* notes 41-49 and accompanying text.

Managers must be informed about their systems' vulnerabilities and must make informed choices about which security provisions to implement and how to enforce them. As the risk of harm increases, managers will be expected to use greater care in protecting systems and verifying the effectiveness of security measures. In general, a manager's duty may be defined as a duty to select and implement security provisions, to monitor their effectiveness, and to maintain the provisions in accordance with changing security needs.

Since security features hinder system access and users want systems that are easily accessible, there are conflicts between the need for security and the desire for ease of use. For example, if passwords are hard to remember, users are likely to write them down, making the passwords accessible to potential intruders. Even on the occasion of substantial harm due to the activities of a network intruder,[108] users caution against overreacting to real or perceived threats in ways that jeopardize a system's usefulness.[109] This "cost" in the ease of using computer systems should be considered in determining whether a manager has exercised reasonable care.[110] However, despite this legitimate concern for ease of use, it is apparent from a legal standpoint that managers should err on the side of caution.

A. *Selecting and Implementing Security Provisions*

To select the right combination of security features, managers must be familiar with the operating systems (control programs that regulate the use of all system resources), the applications software (programs that accomplish specific tasks for users), and the interactions between operating system and application software.[111] Managers configure computer systems for their organizations from vendor-provided options and organization-developed enhancements. Thus, managers have a responsibility to select the right combination of parameters and options for their environments prior to their implementation.

1. Selection and Implementation Choices

Knowing that their products will be used in a variety of environ-

[108] *See generally* Spafford, *supra* note 14, at 678.

[109] King, *Overreaction to External Attacks on Computer Systems Could Be More Harmful Than the Viruses Themselves*, The Chronicle of Higher Educ., Nov. 23, 1988, at A36, col. 1.

[110] *See* Agranoff, *supra* note 28; *supra* notes 41-49 and accompanying text.

[111] *See generally* 2 M. Wofsey, Advances in Computer Security Management 1-37, 143-59 (1983).

ments, vendors generally provide customization options which may be specified at installation time, that permit systems managers to tailor systems to their organization's needs.[112] In order to facilitate installation, however, vendors often configure systems with default values for parameters for user priorities, resource use limits, job accounting, and file protection. Default configurations typically disable available security features, and master accounts typically have default passwords such as "system" or "test." Intruders usually try default user account and password values first. Therefore, a manager will be expected to understand what the default values are and what they imply for security, choose the appropriate set of options, and replace default passwords with secure ones. The choices a manager makes must also be documented. Without such documentation, a computer manager's successor is likely to inherit a poorly secured system. Consequently, he will be unaware of its vulnerabilities.[113]

One kind of option in many systems consists of "backdoor entryways left over from software development."[114] These paths facilitate software development by making debugging easier. One such path, the DEBUG command for verifying receipt of mail at a network node, was used by the Internet intruder. The command permits the sender to invoke commands at the recipient node. The Internet intruder took advantage of this flaw to transmit commands that would propagate unauthorized programs.[115] Although backdoor entryways may be useful and necessary for initial maintenance and debugging, managers should disable such features before making systems available to their users. Vendors should document such features for customers so they can make informed choices to enable them to plan for their use only under controlled operating conditions.

2. User Education

Since the line between use and misuse of computer systems may be hard to discern, system managers have a duty to explain to their users how the application systems are intended to be used and what restrictions apply to each user. A manager's explanation to users should include written documentation.[116] In addition to application

[112] M. MURPHY & X. PARKER, HANDBOOK OF EDP AUDITING § 27-20 (2d ed. 1989).

[113] See Morris & Thompson, *Password Security: A Case History*, 32 COMM. OF THE ACM 594, 596 (1979), for a list of easily guessed passwords.

[114] Stoll, *supra* note 13, at 493.

[115] Spafford, *supra* note 14, at 678-79.

[116] McGuire, *Product-Use Instructions: How to Evaluate Them in Manufacturer*

documentation, systems managers should make clear to their users "rules about what is acceptable and unacceptable conduct when using the system."[117]

3. Access Control

Managers must be aware of the nature of the information in system files and the extent of the security that is appropriate for different kinds of files. All files should be subject to periodic backup so that if they are damaged by an intruder, files can be restored readily.[118] Additionally, managers must know which individuals are authorized, for what type of access, to what information, and under what conditions. For example, inventory clerks might be authorized for access only during their assigned shift with update access to inventory quantities but read-only access to price data.[119]

Moreover, the concern with access authorization should extend to documentation about systems.[120] With sufficient documentation available to them, clever intruders may discover how to masquerade as legitimate users.[121]

Managers should be responsible for implementing procedural and programmed security provisions so that the desired level of control is achieved in environments where there are many users, where their passwords are vulnerable to exposure, and where there are software errors.[122] In addition, an important aspect of security implementation is separating incompatible functions of authorizing access privileges, specifying access privileges for individuals to the system, and reviewing records of computer access for patterns of fraudulent activity.

Negligence, 11 J. PROD. LIAB. 293, 293-97 (1988) (discussing manufacturers' product-use instructions). Systems managers could be thought of as manufacturers for the purpose of designating the content of user documentation.

[117] Samuelson, *supra* note 12, at 669. Acceptable conduct for computer users means, for example, their (1) using only those computer accounts authorized for their use and using them only for the purposes for which they were authorized, (2) making appropriate use of system-provided protection features such as passwords and not attempting to subvert passwords or other restrictions on account use, and (3) accessing the files of others only with express permission for authorized purposes.

[118] R. WEBER, EDP AUDITING: CONCEPTUAL FOUNDATIONS AND PRACTICE 294 (1988).

[119] *Id.* at 515.

[120] *Id.* at 295.

[121] D. PARKER, CRIME BY COMPUTER 59-70 (1976) (access to system documentation enabled outsider to pose as Pacific Bell employee and embezzle equipment from the company).

[122] Murray, *Computer-Related Crime and Auditing in the Nineties*, II THE EDP AUDITOR J. 25, 25-30 (1990).

Separating these functions means vesting each one in a different individual or group of individuals.

Access control[123] is typically implemented through user identification codes ("user IDs") corresponding to user accounts, together with their associated passwords. User IDs identify individuals, while passwords allow the individuals to validate themselves as the owners of the user IDs. Thus, knowledge of user IDs and passwords may permit intruders to masquerade as authorized individuals. Since user IDs are generally not subject to even casual protection, knowledge of passwords is effectively all that intruders require to gain system access.

Historically, users have been careless with passwords. They choose obvious combinations such as their initials or their spouses' names and write them down in obvious places.[124] As a result, managers must force periodic password changes so that intruders cannot guess or detect passwords even with repeated attempts. As intruders become more sophisticated in deciphering passwords, managers must take more elaborate security steps, such as encrypting passwords so that intruders are unlikely to uncover them even with unlimited computer time at their disposal.[125]

A crucial aspect of implementing computer security is maintenance of control over the content of all software on the system.[126] Software integrity is vital because if intruders can corrupt software, especially control programs with system-wide access and privileges, they can manipulate systems more easily.[127] Customary procedures for assuring software integrity include: restricting access to program code solely to the employees responsible for implementing and running it;[128] requiring separate developmental and production software

[123] See R. WEBER, *supra* note 118, at 309-56, for a discussion of access control.

[124] Observation of the daily security coding in a bank's wire transfer room enabled a consultant to make an unauthorized wire transfer of $10.2 million from Security Pacific National Bank. *FBI Arrests Suspect In Bank Funds Theft and Finds Diamonds,* Wall St. J., Nov. 7, 1978, at 24, col. 3.

[125] *See* Morris & Thompson, *supra* note 113, at 594. The authors describe the need for and the evolution of increasingly sophisticated password security. In addition to encrypting passwords, they recommend forcing users to use less predictable passwords, concealing the list of encrypted passwords, and using time-consuming encryption algorithms. *Id.*

[126] F. GALLEGOS, D. RICHARDSON & A. BORTHICK, AUDIT AND CONTROL OF INFORMATION SYSTEMS 195-96 (1987). Control over software content is important because data integrity depends on programs to do all of what they are supposed to do and nothing else. If programs are changed surreptitiously, then the perpetrators might be able to manipulate organizational data for their own purposes.

[127] R. WEBER, *supra* note 118, at 185-86. For example, privileged system software could be used to gain access to private data that could be sold to competitors.

[128] AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS, STATEMENT ON

libraries;[129] requiring management authorization for program changes and approval for installation;[130] and verifying the legitimacy of production programs on periodic and random bases.[131]

B. *Monitoring Effectiveness*

The manager has a duty to monitor the effectiveness of the operation of security provisions. Monitoring should include verifying that security provisions work as intended and analyzing attempted accesses to identify fraudulent ones. Attempted accesses should be logged for examination and all suspicious activity should be investigated.[132]

Monitoring security effectiveness also encompasses an awareness of the temptations to individuals for fraudulent activity.[133] Individuals with access to computer systems should be screened, and employee attitudes and satisfaction should be monitored.[134] There should be a legitimate grievance procedure for dissatisfied employees — especially those who actively use the system and have access to computer files. The most dissatisfied employee may be an ex-employee or someone about to become an ex-employee.[135] Therefore, managers should immediately implement procedures that deny access to terminated employees.[136] For laid-off employees subject to The Worker Adjustment and Retraining Notification Act of 1988,[137] managers should either deny access privileges altogether or monitor their activities.

Another problem concerning security effectiveness is system failures. Abrupt system failures create opportunities for compromising

AUDITING STANDARDS NO. 55, CONSIDERATION OF THE INTERNAL CONTROL STRUCTURE IN A FINANCIAL STATEMENT AUDIT ¶ 11, at 6 (1988). This statement generally establishes the requirements of an internal control structure comprising the control environment, the accounting system, and control procedures, for the purpose of giving reasonable assurance that transactions are authorized, transactions are recorded accurately, access to assets is permitted only as authorized, and records of assets are compared with existing assets.

[129] *Id.*

[130] *Id.*

[131] *Id.* at 7.

[132] F. GALLEGOS, D. RICHARDSON & A. BORTHICK, *supra* note 126, at 496-97; J. MARTIN, SECURITY, ACCURACY, AND PRIVACY IN COMPUTER SYSTEMS 186-87 (1973).

[133] *See* R. ELLIOTT & J. WILLINGHAM, MANAGEMENT FRAUD: DETECTION AND DETERRENCE (1980).

[134] A. HUTT & S. BOSWORTH, COMPUTER SECURITY HANDBOOK 33-45 (2d ed. 1988).

[135] *Id.* at 41.

[136] *See* Savage, *supra* note 25, at 2 (failure to deny former employee all computer access led to the deletion of payroll information).

[137] 29 U.S.C. §§ 2101-2109 (1988). The Worker Adjustment and Retraining Notification Act provides for employer notification for plant closings and mass layoffs.

systems. When a system crashes, computer operators attempt to restore processing quickly to minimize user inconvenience. If security features impede restoring the system quickly, computer operators may disable access control and forget to restore it when the crisis passes. Managers should have procedures for reviewing system activity associated with restarting failed systems to verify that security is disabled only when absolutely necessary and is quickly restored.[138]

C. *Maintaining Systems*

1. Changing Computing Environments

Managers must take reasonable care to modify security provisions in accordance with changing security needs. The computing environment continually evolves: systems grow in size and in the number of access points; new versions of hardware and software are regularly provided to users; there are increases in the number of users, in the computing competence of individuals and society generally, and in the complexity of systems. Security features appropriate in one environment may be ineffective in another. One event that should always signal the need to reevaluate security features is the implementation of new software or new versions of existing software. A manager is tempted to implement new software in the same manner as the old software. The risk is that this default approach may lead to unanticipated vulnerabilities.[139]

2. System Flaws

Even if vendors follow the best hardware and software development practices, they cannot guarantee error-free systems. It is a manager's responsibility to decide, primarily through testing, whether systems and subsystems are sufficiently error-free so that if they were installed, their use would not lead to unpredictable or destructive behavior. As far as possible, managers should test new products in isolation so that if the products are corrupted,[140] the damage can be confined to the test system. To minimize the likelihood of acquiring

[138] R. WEBER, *supra* note 118, at 186. Systems are vulnerable just after failures when the need to get jobs running overrides the need to maintain established control procedures.

[139] F. GALLEGOS, D. RICHARDSON & A. BORTHICK, *supra* note 126, at 352-53. For example, the vendor may change default values for security-related features or change the features themselves. Vendors typically help systems managers understand revisions by including lists of feature changes in documentation for revised software.

[140] See Tuck, *The Aftermath of the Virus*, I THE EDP AUDITOR J. 9, 10 (1989), for an account of the purchase of corrupted software from a commercial vendor.

maliciously corrupted software, managers should buy software only from authorized sources.[141]

Software inevitably has flaws because no known developmental technique guarantees error-free software.[142] The more complex the software, the more likely it is to contain errors. Verifying the absence of intentional errors is even more difficult.[143] Consequently, vendors are continually patching software when fatal or costly errors come to their attention. System managers should report these problems promptly to vendors. When vendors distribute software patches for correcting software errors, system managers should implement them only after thorough testing. Clifford Stoll attributes the reluctance to publicize patches for security functions "to the paranoia surrounding these discoveries . . . and [to] the lack of channels to spread the news."[144] Vendors have a responsibility to document security-related patches and to take positive steps to distribute them to customers, whether they are purchasers or lessees.

CONCLUSION

There is considerable tension among computer users between the need for free access to computers and concerns for security. The academic community in particular has warned against overreaction to recent incidents of computer abuse and has stressed the need for continued openness and accessibility of computer networks.[145] A balance between these two concerns is clearly needed even though the potential for serious harm, where software is infected or sensitive information is exposed, tips the balance in favor of security.

Systems managers cannot be expected to be insurers of security, nor can they be responsible for all problems and wrongful acts by third

[141] Denning, *supra* note 21, at 238.

[142] See Fetzer, *Program Verification: The Very Idea*, 31 COMM. OF THE ACM, 1048, 1049-63 (1988), for a discussion of the difficulties inherent in verifying the correctness of computer programs. Fetzer states that program performance cannot be guaranteed because it is a function of the interaction of ill-defined components, i.e., software, firmware, and hardware, and is thus probabilistic rather than deterministic. Repeated tests give only inductive evidence of reliability, which is insufficient to prove program correctness. *Id.* at 1061.

[143] Thompson, *Reflections on Trusting Trust*, 27 COMM. OF THE ACM 761, 762-63 (1984). Thompson explains how to change a compiler to make it deliberately miscompile source code whenever it encountered a particular pattern. With this technique, intentional unauthorized features could be introduced into programs. This example demonstrates Thompson's point that no amount of source-level verification will identify all errors, with the result that well-installed bugs will be almost impossible to detect.

[144] Stoll, *supra* note 13, at 493.

[145] King, *supra* note 109.

parties. Managers will, however, be expected to use reasonable means to secure computer systems and protect information — especially when there is significant potential for harm to innocent third parties. What constitutes reasonable care will vary with the circumstances of each case and will change over time. Systems managers must be aware of the potential liability and should document all security-related features and their effectiveness.