Santa Clara University School of Law

Santa Clara High Technology Law Journal

Volume 5 | Issue 1 Article 4

January 1989

Failure to Prepare: Who's Liable in a Data Processing Disaster?

Dan L. Burk

Laurence H. Winer

ARTICLES

FAILURE TO PREPARE: WHO'S LIABLE IN A DATA PROCESSING DISASTER?

Dan L. Burk†
Laurence H. Winer††

INTRODUCTION

In December 1986, fire in the building housing the Boston offices of Putnam Cos., cut off power to the investment management firm's computer center.[1] In June 1987, floods in Chicago inundated the data processing center at Household Finance Corp., leaving fish swimming through the company's computers.[2] In October 1987, an earthquake in Los Angeles paralyzed the data processing center of California Federal Savings and Loan, separating the bank's numerous branches from customer account records.[3] In each case, a potentially crippling disaster was avoided by moving data processing operations to an alternate computer site. Each firm had previously prepared a computer disaster recovery plan.

What if no contingency plans had been made? Modern corporations, dealing in every service from banking to utilities, have become increasingly dependent on their electronic data processing systems.[4] Loss of those systems can stall the critical functions of a

† B.S., Brigham Young University, 1985; M.S., Northwestern University, 1987. Mr. Burk is a J.D. candidate for May, 1990 at the Arizona State University College of Law.

†† J.D., Yale University, 1977; Ph.D., Boston University, 1973; Professor, Arizona State University College of Law; Affiliated Faculty, ASU Center for the Study of Law, Science, and Technology [CeSLaST].

The authors wish to acknowledge that research for this paper was supported in part by an unrestricted grant from SunGard Data Systems Inc., which is mentioned in the text.

1. Koselka, *Blue-chip Back-up*, FORBES, Jan. 26, 1987, at 80.

2. Bozman, *It Was a Dark & Rainy Night*, COMPUTERWORLD, Feb. 29, 1988, at 14, col. 1. *See also* Robbins, *Disaster Recovery: Trial by Flood*, INFOSYSTEMS, Jan. 1988, at 40.

3. *Back-up Site Allows Quick Recovery*, SAVINGS INST., Dec. 1987, at 136 [hereinafter *Back-up Site*].

4. For an overview of various applications, see generally *Industry by Industry Technology Forecast*, DATAMATION, Jan. 15, 1988, at 58-92.

firm, destroy vital records, and cause costly delays.[5] A nine hour shutdown of one bank's computer facilities reportedly caused losses of over $1,000,000.[6] A computer system failure at the Bank of New York cost the bank $4,000,000 during the several days required for repair.[7] Electronic data processing has brought with it many advantages, but also a special type of vulnerability: records which consist of no more than an electrical impulse are easily destroyed.[8]

Business insurance may cover the cost of computer hardware replacement, or even the losses incurred while a computer is down and business is interrupted.[9] However, even this safeguard may have become inadequate.[10] A recent University of Texas study indicates that 75% of computer dependent businesses would suffer crippling losses if deprived of their electronic data processing systems for more than 14 days.[11] Some firms might be out of business within a week.[12] A previous study conducted by the University of Minnesota suggested that certain corporations would suffer permanently disabling loss after only 48 hours without operational com-

---

5. *See Safety In Numbers*, COMPUTERWORLD FOCUS, April 6, 1988, at 40 (1986 projection of electronic data processing disaster costs).

6. West, *Disaster Prevention and Recovery Options for Check Processing*, MAG. BANK ADMIN., June 8, 1985, at 64.

7. Betts, *Bank Blames Nightmare on Software Flop*, COMPUTERWORLD, Dec. 16, 1985 at 1, col. 3; Goldberg, *DP Nightmare Hits NY Bank*, COMPUTERWORLD, Dec. 16, 1985, at 1, col. 3. These losses were caused by software failure rather than some natural disaster, but illustrate what may occur when businesses are unexpectedly deprived of their electronic data processing capability.

8. *See* Carter, *Loss of Memory: An Unforgettable Experience*, ACCT., March 1987, at 144.

9. Insurance is available to cover the cost of replacing damaged computer hardware and software, as well as costs of extra expenses such as moving to an alternative data processing facility. *See Rating Your Risks*, DATAMATION, Feb. 1, 1987, at 62; *see also* Passori, *Contingency Planning Options Protect Corporate Data Assets*, COMPUTERWORLD, Jan. 27, 1986, at 74, col. 4. Business interruption insurance may cover lost revenues directly related to data processing.

However, determining exactly which losses are within the coverage of such insurance may be a difficult and unsatisfactory process for all parties involved. *See also generally*, Detamore, *Functional Value vs. Actual Cash Value in Partial Loss Settlements*, 50 INS. COUNS. J. 332 (1983); Hoey, Ozog & Schaefle, *Management of a Complex Business Interruption Case*, 52 INS. COUNS. J. 669 (1985).

10. Uninsured intangible losses such as cash flow interruption, loss of market share, loss of competitive edge, or decrease in customer confidence may cause the greatest damage to a business that unexpectedly loses its electronic data processing capacity. S. CHRISTENSEN & L. SCHKADE, FINANCIAL AND FUNCTIONAL IMPACTS OF COMPUTER OUTAGES ON BUSINESS, CRIS-87-01, at 10 (1987) (Center for Research on Information Systems).

11. *Id.*, at 11. *See also* Wall, *Few Firms Plan Well for Mishaps that Disable Computer Facilities*, Wall St. J., May 31, 1988, at 27, col. 4.

12. Wall, *supra* note 11, at col. 4.

puter facilities.[13] Because of such studies, corporate officers have begun to realize that their corporation's electronic records are perhaps their firm's most valuable asset — and their most vulnerable.[14]

In the face of such vulnerability, many firms are investing in a different sort of insurance. Corporations that rely heavily on electronic data processing operations have begun to build or lease alternate computer sites for use during a disaster.[15] Highly publicized events such as the computer disasters discussed above have alerted many corporate executives to their firms' vulnerability.[16] New services have appeared to supply the disaster recovery market; these services have been widely discussed in the popular press.[17] Federal agencies have begun to take notice of this problem,[18] and support groups have sprung up to aid the managers who prepare and implement computer disaster recovery plans.[19]

Despite the widespread discussion of computer disaster recovery, many corporate directors and officers remain oblivious or hostile to discussion of such plans.[20] Tales of information systems managers whose prophecies of doom went unheeded by corporate executives are well known in data processing circles.[21] Often, executives are unwilling to commit time or money to prepare for a computer disaster — yet the disaster, if it strikes, could close the doors of their business forever.[22] As one standard text on computer audit

---

13. *Regulations Demand Sold Planning For Disaster Recovery*, SAVINGS INST., Sept. 1987, at 115 [hereinafter *Regulations*].

14. *See* Wall, *supra* note 11, at col. 5 (" '. . . the value of the information (in the computer) could very well be worth several times the value of their hardware, software, and building,' says Steven Christiansen, a researcher at the University of Texas."). *See also* Passori, *supra* note 9, at 73, col. 1; Usdin, *Like It or Not, Plan for Disaster Recovery*, OFFICE, March 1987, at 90.

15. *See* Wall, *supra* note 11, at col. 5; *see also* Elliott, *A New Kind of Recovery Service*, ACCT., Feb. 1986, at 121 (description of British disaster recovery industry).

16. Rohm, *That's All That's Left*, INFOSYSTEMS, Feb. 1987, at 48.

17. *See*, e.g., Koselka, *supra* note 1; Marbach, Leech & Gibney, *Now, Computer Paramedics*, NEWSWEEK, Dec. 28, 1987, at 38; Wall, *supra* note 11, at col. 5.

18. *See infra* notes 115-133 and accompanying text.

19. Ludlum, *Contingency Groups Spring Up*, COMPUTERWORLD, Sept. 7, 1987, at 77, col. 2; Robbins, *Disaster Recovery: No Longer the Loneliest People in the World*, INFOSYSTEMS, June 1987, at 38.

20. *See* Dugan, *Disaster Recovery Planning: Crisis Doesn't Equal Catastrophe*, COMPUTERWORLD, Jan. 27, 1986, at 67, col. 2; at 69, col. 1. *See also* Wierzbicki, *Preparing for Catastrophe: You Can't Dodge the Bullet*, COMPUTERWORLD, May 12, 1986, at 58, col. 1 (interview with Comdisco president Raymond Hipp).

21. *See* Pedigo, *Disaster Recovery: Making Plans That Could Save Your Company*, COMPUTERWORLD, May 12, 1986, at 49, col. 1; Stamps, *Disaster Recovery: Who's Worried?*, DATAMATION, Feb. 1, 1987, at 60.

22. *See generally* Carter, *supra* note 8; *see also supra* notes 9-12 and accompanying text.

observes in discussing disaster recovery:

> In evaluating the threat of computer disaster, consider the following parallels: Would it be prudent to leave unsecured such physical documents as the corporate general ledger, journals, subsidiary ledgers, and source documents? Would it be standard practice to leave millions of dollars in cash or negotiable instruments unprotected, in one room? . . .
>
> The failure to institute adequate safeguards in each of these cases would be downright negligent. However, in general, information assets are left relatively unsecured in centralized computing facilities. . . . In effect, the "corporate memory" of the organization is being exposed to accidental loss. . . .[23]

What duties do corporate executives owe their corporations, shareholders, depositors, creditors, or customers regarding computer disaster recovery? This paper examines whether failure to take adequate precautions for computer disaster recovery constitutes negligence not only in the everyday sense, but in the legal sense as well. Such legal negligence might leave corporations, directors, and officers liable for certain damages suffered due to inaccessibility or loss of records and data processing capacity during a computer disaster. Part I of this paper discusses the disaster recovery options available to corporations. Part II outlines corporate liability under several statutes requiring computer disaster preparedness. Part III discusses the common law duties of corporations, directors, and officers as applied to this topic. Finally, Part IV suggests a theory of tort liability that might be applied to losses in computer disaster, and indicates areas to which this theory might extend.

I. PREPARING FOR COMPUTER DISASTER

A. *Economic Considerations*

Preparing a computer disaster recovery plan, like making any other business judgment, requires that corporate officers and directors weigh several competing economic considerations.[24] Computer problems come in many sizes and shapes. Generally, the cost of a precautionary measure will be a function of the frequency and se-

---

23. F. GALLEGOS, D. RICHARDSON, & A. BORTHICK, AUDIT AND CONTROL OF INFORMATION SYSTEMS 96 (1987).

24. *See* West, *supra* note 6, at 65; Sporck, *Without a Records Recovery Plan, Start From Square One*, OFFICE, June 1987, at 57; *see also* Murray, *How Much is Enough? Expert Says Security Efforts Should Pay, Not Cost*, COMPUTERWORLD FOCUS, April 6, 1988, at 30, col. 1.

verity of the disaster guarded against.[25] Some precautionary measures may be taken to avert mishaps; other measures must be designed to speed recovery from an unavoidable disaster. The size of the firm, its dependence on electronic data processing, and the resources available to commit to disaster preparedness must all be considered. In addition, legal and regulatory requirements must be considered.[26]

Certain computer mishaps are fairly likely to occur: data entry mistakes, a power surge, or a minor software error might be common examples of this type of problem.[27] These problems are disruptive, but rarely result in thorough devastation.[28] They can usually be dealt with by relatively inexpensive preventive measures. For example, protective devices are commonly used to prevent current fluctuations from destroying electronic data.[29] Backup copying of data remains the least expensive but most effective form of electronic data protection;[30] even offices with small data processing needs quickly learn the importance of frequently updating duplicate copies of important files and software.[31] Indeed, more sophisticated forms of computer protection rely largely on the simple measure of creating backup files.[32]

Other computer mishaps may be either too improbable or too costly to prepare for; falling meteors or a thermonuclear terrorist attack might fall into this category. Generally, the resources expended in preventing this type of disaster will outweigh any benefit

---

25. *See* Sporck, *supra* note 24, at 57; West, *supra* note 6, at 65; *see also* Murray, *supra* note 24, at col. 4.

26. *See infra* discussion in Part II.

27. *See Murray*, *supra* note 24, at col. 4; *Safety, In Numbers*, *supra* note 5.

28. Disruptions such as major software failure, of course, can be extremely costly, as in the instance reported *supra* at note 7. However, even in such instances the hardware and data processing site remain intact for recovery.

29. *See* Kolodziej, *The Ins and Outs of UPS*, COMPUTERWORLD FOCUS, April 6, 1988, at 26; Rhodes, *An Electifying Situation*, INFOSYSTEMS, Dec. 1986, at 48.

30. *See* Robbins, *Disaster Recovery: Don't Stuff Your Backup Tapes in a Box and Stash Them in a Cave*, INFOSYSTEMS, Aug. 1987, at 18; *see also* Innovation Data Processing v. IBM, 585 F. Supp. 1470, 1473 (D.C.N.J. 1984) (recognizing importance of back-up).

31. Robbins, *supra* note 30, at 18. Even the simple precaution of data backup requires costs and benefits to be weighed. Firms must weigh benefits against inconvenience in choosing how often to update backup files. Electronic vaulting technologies allow virtually continual instantaneous file backup, but the cost is often prohibitive. *See* Schreider, *If You Can't Afford to Wait. . .*, COMPUTERWORLD SPOTLIGHT NO. 48, July 11, 1988, at S-11.

32. Schreider, *supra* note 31, at S-11. *See also* Elliott, *supra* note 15, at 122; Sherman, *Is Your Vital Information Protected?*, ADMIN. MGMT., June 1986, at 50, 51; Whitehead & Conyers, *Survival in a Computer Environment — The Synergistic Approach*, ARMA REC. MGMT. Q., Jan. 1988, at 12.

gained.[33] This may not be true, of course, for certain large firms that are highly dependant on uninterrupted data processing. American Airlines, for example, recently completed an underground computer center with sophisticated personnel security screening devices.[34] The center has a food stockpile as well as a fuel supply to power its own electrical generators.[35] This center houses the nexus of the Sabre computer network, which every hour processes thousands of airline reservations from all over the world.[36] A handful of other firms have constructed similar "disaster proof" sites, but such measures are the exception, rather than the rule.[37]

Computer disaster recovery plans deal generally with protection between these two extremes.[38] Fire, floods, earthquakes, and tornadoes strike infrequently, but have a devastating impact when they do strike. Computer dependent firms with sufficient resources may adopt strategies to enable them to recover from a disaster too costly to prevent.[39] Small firms may not have this option; often they must rely on inexpensive preventive measures, and take their chances with the threat of large scale disaster. Larger corporations, with more resources at stake, also have more resources to commit to developing disaster recovery measures. These measures generally involve off-site storage of frequently updated files and programs, as well as provisions to use duplicate critical computer functions off-site if a disaster strikes.[40] Such a plan ensures not only that electronic records are preserved through a disaster, but that they are accessible afterward. These measures may be implemented in several ways.

B. *Disaster Recovery Options*

Hot Sites — A hot site is a fully equipped computer facility to which data processing operations may be transferred in the event of

33. *See* Murray, *supra* note 24, at 30; Sporck, *supra* note 24, at 58; West, *supra* note 6, at 65.

34. *See* Marbach, Leech & Gibney, *supra* note 17.

35. *Id.*

36. *See* Stamps, *supra* note 21, at 64.

37. *Id.*

38. *See* West, *supra* note 6, at 65.

39. The considerations discussed here are also weighed in determining the scope and cost of insurance against a disaster. Thus, implementation of adequate disaster precautions will often save a firm money on disaster insurance premiums, simply by eliminating negative factors that an insurer will consider. *See Rating Your Risks*, *supra* note 9.

40. *See generally* Ainsworth, *Contingency Options Abound With Off-site Backup Facilities*, COMPUTERWORLD, May 12, 1986, at 56, col. 1.

a disaster.[41] This disaster recovery option has been perhaps the most highly publicized.[42] Several firms offer hot site subscriptions commercially; the largest of these are SunGard Data Systems Inc. and Comdisco Inc. Each firm maintains several operational computer facilities in different areas of the United States, Canada and Europe.[43] In addition, a number of smaller disaster recovery service firms offer more limited computer facilities locally.[44] Corporations subscribe to whichever service maintains equipment compatible to the corporation's own.[45] SunGard, with about 400 customers, caters primarily to larger corporations requiring large capacity mainframe computers.[46] Comdisco, with about 700 customers, provides backup facilities to mid-sized firms with more moderate computer hardware needs.[47]

Hot-site subscriptions generally are not recommended for smaller corporations or firms with little need for telecommunications.[48] Part of the reason is the price; firms subscribing to these services pay a monthly fee which may range from $1,500 to $100,000.[49] The amount paid depends upon the type of equipment and service desired.[50] Subscribing firms also pay a disaster declaration fee of $10,000 to $50,000 in order to gain access to the facility in a disaster; additional fees are assessed while the facility is actually in use.[51] The disaster recovery service firms typically contract with several corporations in the same area for use of the same sites.[52] In an area wide disaster, some services assign facilities on a "first come, first served" basis; others guarantee equal access and shared

41. Hot sites generally contain one or more mainframe computers, peripheral devices, and necessary telecommunication equipment. *See* Ainsworth, *supra* note 40, at 56, col. 3; *see also* Elliott, *supra* note 15, at 122. Some commercial services have begun offering "warm sites" containing everything but the mainframe. *See* Ainsworth, *supra* note 40, at 57.

42. *See supra* notes 1-3 and accompanying text.

43. *See Disaster Prevention and Recovery*, COMPUTERWORLD SPOTLIGHT NO. 48, July 11, 1988, at S-14 [hereinafter *Disaster Prevention*].

44. *Id.*

45. *See* Scisco, *Approach Your Hot Site as Home Away From Home*, COMPUTERWORLD SPOTLIGHT NO. 48, July 11, 1988, at S-5, col. 1.

46. *See Disaster Prevention*, *supra* note 43.

47. *Id.*

48. *See* Robbins, *supra* note 2, at 45.

49. *See* Marbach, Leech & Gibney, *supra* note 17; Wall, *supra* note 11.

50. *See Regulations*, *supra* note 13, at 117; Stamps, *supra* note 21, at 63. The services offered may include even meals and toothbrushes for displaced personnel. *See* Raimondi, *Hot Sites: Disaster Plan Douses Flames*, COMPUTERWORLD, Nov. 17, 1986, at 6, col. 3.

51. Raimondi, *supra* note 50 at 1, col. 2.

52. *See* Bozman, *supra* note 2; Bozman, *DP Sites Drip-dry in Chicago*, COMPUTERWORLD, Aug. 24, 1987, at 1, col. 2; at 4, col. 2.

usage.[53] During 1987 flooding in the Chicago area, three of Comdisco's customers declared disasters. The Comdisco facilities in the area were adequate for only two; tapes and personnel from the third were airlifted to another site in Pennsylvania.[54]

Corporations with highly specialized needs may also find hot site subscriptions to be undesirable. Specialized equipment, such as the check processing machinery used by banks, may not be available at commercial hot sites.[55] Security at a commercial hot site may be inadequate for some firm's needs.[56] The inconvenience of moving records and personnel to a somewhat distant hot site may also be undesirable, although remote access telecommunications have begun to alleviate this problem.[57] The last problem has been addressed to some extent by service firms offering mobile hot sites, which they drive to the parking lot of the subscriber's damaged computer center.[58]

Cold Sites — A cold site, or shell, is simply a facility ready for the installation of computer hardware.[59] A corporation may subscribe to a cold site service in much the same manner it would subscribe to a hot site; both types of service are offered by SunGard and Comdisco.[60] The costs for cold site subscription, however, are considerably less; no expensive computer equipment is maintained in readiness at the facility.[61] In an emergency, the subscribing corporation must contact its computer hardware vendor to deliver duplicate equipment to the cold site; the necessary air conditioning, temperature control, electrical cables, and telecommunication hook-ups are available at the cold site.[62] This option is attractive because its cost is minimal until a disaster actually occurs. In addition, some firms may have need of highly specialized equipment that would not be available at a commercial hot site; these corporations may tailor the equipment at the cold site to their needs, rather than maintain a private facility year round.[63]

However, two serious disadvantages to cold sites prevent most corporations from seriously considering this option to computer

53. Bozman, *supra* note 52, at col. 3.
54. *Id.*
55. *See* West, *supra* note 6, at 72.
56. *See id.*
57. *See id.*; *see also* Ainsworth, *supra* note 40.
58. *See* Rohm, *supra* note 16, at 46.
59. Ainsworth, *supra* note 40, at 57.
60. *See Disaster Prevention*, *supra* note 43, at S-14.
61. *See Regulations*, *supra* note 13, at 116.
62. Passori, *supra* note 9, at 73, col. 3.
63. *See infra* notes 88-91 and accompanying text.

disaster recovery. First, a recovery plan that centers around a cold site cannot be tested.[64] No equipment is available at the site, until ordered in an actual disaster. Computer personnel will therefore have no experience reestablishing full data processing operations at the new site, under time pressure. Far more prohibitive, though, is the delay in delivery of the duplicate equipment to the site. Ten to twenty-seven days may be required for a vendor to deliver computer hardware to the cold site.[65] In an actual emergency, loss of data processing for this period of time would seriously cripple or destroy most corporate operations.[66]

Reciprocity Agreements — Some corporations may choose not to contract for disaster recovery sites, but may instead enter into a reciprocity agreement with another firm.[67] Under such an agreement, each firm agrees to allow the other to use its computing facilities in the event of a disaster.[68] This "buddy system" is possible only if a corporation can find another that uses the same computer hardware and software.[69] Reciprocity agreements are attractive because they offer corporations a measure of security without the subscription and disaster declaration fees of commercial hot or cold site contracts.[70] These agreements have traditionally been the most common type of disaster recovery plan.[71]

In practice, however, relying on a reciprocity agreement may be tantamount to relying on no disaster recovery plan at all.[72] Such agreements assume, first, that at least one of the firms entering the agreement will be unaffected by whatever disaster overtakes the other. More important, these agreements assume that the computer facilities at the unaffected firm have sufficient operating capacity to accommodate the demands of both firms.[73] This is rarely the case, and where demand for computer time is greater than can be met, the "nonresident" firm's needs may have to wait.[74] Maintaining compatibility between the data processing operations at each firm

64. Passori, *supra* note 9, at 73, col. 3.

65. *See Regulations*, supra note 13, at 116; West, *supra* note 6, at 72.

66. *See supra* notes 10-13 and accompanying text.

67. *See* Ainsworth, *supra* note 40, at 56.

68. *Id. See also* Passori, *supra* note 9, at 73, col. 1.

69. *See* Chung, *Contingency Planning: A Funds Transfer Perspective*, MAG. BANK ADMIN., Sept. 1987, 16, 18.

70. *See* Usdin, *supra* note 14, at 90.

71. Melia, *Auditor Devises Disaster Plan*, SAVINGS INST., Sept. 1987, at S-72.

72. *See* Whitehead & Conyers, supra note 32, at 12. *See also* Wierzbicki, *supra* note 20, at 58, col. 4.

73. *See* Whitehead & Conyers, *supra* note 32, at 12; Wierzbicki, *supra* note 20, at 58, col. 4; *see also* Stamps, *supra* note 19, at 63; Usdin, *supra* note 14, at 90.

74. *See* Wierzbicki, *supra* note 20, at 58, col. 4; *see also* Usdin, *supra* note 14, at 90.

may also become a serious problem.[75] Experts in disaster planning charge that reciprocity agreements offer only a false sense of security; the agreements are a panacea for corporations wishing to avoid the unpleasant realities of disaster recovery planning.[76] Nonetheless, such agreements may be the only viable option for small firms.[77]

Service Bureaus — Service bureaus perform data processing jobs for a fee.[78] Corporations without internal data processing capability routinely send such work to a service bureau.[79] Corporations that normally have internal data processing capability sometimes plan to send data processing out to a service bureau should a computer disaster strike.[80] This approach avoids the costs of subscription to a hot site or the cost of maintaining a private backup facility. The only costs are the fee paid to the service bureau for work done after a disaster actually occurs.

However, the advantages of internal data processing capability are lost when processing is turned over to an outside service. Corporations with internal data processing usually purchased their own computers because the volume of work done makes buying the equipment cost effective. When that volume of work is sent to an outside service, for even a short time, costs rapidly mount.[81] In addition, reliability, control, and secrecy may be sacrificed by turning data processing over to a service bureau. A corporation accustomed to performing its own data processing may not have previously worked with a service bureau. The bureau will be unfamiliar with that corporation's specialized needs, causing confusion, error, and delay.[82] These factors make reliance on service bureaus a more worthwhile option only for smaller firms with more limited means and needs.[83]

Private Facilities — Corporations such as Motorola and BankAmerica have chosen the most direct approach to disaster re-

---

75. *See* Usdin, *supra* note 14, at 90.

76. *See* Scisco, *No Such Thing as a Small Mishap*, COMPUTERWORLD SPOTLIGHT NO. 48, July 11, 1988, at S-1, S-6, col. 4; *see also* Wierzbicki, *supra* note 20, at 58, col. 4; Usdin, *supra* note 14, at 90.

77. *See* Usdin, *supra* note 14, at 90.

78. *See* Whitehead & Conyers, *supra* note 32, at 8, 9.

79. *Id.*; *see also* Passori, *supra* note 9, at 74, col. 1.

80. *See* Passori, *supra* note 9, at col. 1.

81. *Id.*

82. *Id.*; *see also* Scisco, *supra* note 76, at S-6, col. 5.

83. *See* Scisco, *supra* note 76, at S-6, col. 5.; *See also* Whitehead & Conyers, *supra* note 32, at 8, 9.

covery: they have built their own duplicate backup facilities.[84] This approach assures that the alternate facilities are tailored to the corporations needs. The problem of "first come first served" availability is also avoided by such an approach. However, the cost of building and maintaining a duplicate facility against a somewhat remote catastrophe can be prohibitive.[85] This option is therefore best suited to firms with extensive resources, particularly where their computing needs are so specialized as to preclude subscription to a general purpose commercial facility.[86]

Even large corporations, though, have difficulty justifying the expense of maintaining an idle facility against the somewhat remote contingency of a debilitating data processing catastrophe.[87] Idle equipment in a large organization tends to become occupied for one project or another; when this occurs, the facility may not be available during the emergency for which it was built.[88] Some corporations have therefore attempted to defray the expense of maintaining alternate facilities by banding together and maintaining the facility as a consortium.[89] Similarly, the cost of a private facility may also be lessened by contracting it out as a hot site for other firms.[90] This approach is perhaps the most viable alternative to a commercial hot-site subscription, although it may be subject to the same compatability concerns as reciprocity agreements.[91]

C. *Disaster Recovery Agreements*

Many of the considerations embodied in the written agreement for a disaster recovery site must also be weighed when evaluating a corporation's options.[92] The provisions of the agreement a firm enters will cover more than simply fees, particularly if the agreement concerns a commercial recovery service subscription. These agreements will define the scope of services provided: the type of site, the equipment and personnel available, transportation, or other ar-

84. *See* Stamps, *supra* note 21, at 63; Wall, *supra* note 9, at 32, col. 5.

85. *See* Passori, *supra* note 9, at 73, col. 1.

86. *See* West, *supra* note 6, at 72.

87. *See* Passori, *Protecting Your Corporate Computer Assets*, DISASTER RECOVERY J., July/Aug./Sept. 1988, at 30, 34.

88. *See* Ainsworth, *supra* note 40, at 56, col. 1; Wierzbicki, *supra* note 20, at 58, col. 4.

89. *See Regulations*, *supra* note 13, at 116.

90. *See Back-up Site*, *supra* note 3, at 137; *Selling Disaster Recovery Services Helps Pay Bills*, SAVINGS INST., Sept. 1987, at 115.

91. *See* Stamps, *supra* note 21, at 63; Passori, *supra* note 87, at 34.

92. *See* Ainsworth, *supra* note 40, at 57, col. 4.

rangements as described above.[93] If the agreement is a hot site subscription, it should make provisions for testing, particularly if equipment or software is upgraded or replaced.[94] The agreements will also define what may constitute a disaster, how soon and how long a subscriber may use the facilities in the event of a disaster, and the number of subscribers that may contract to use the same site.[95] In addition, the agreement may disclaim the service firm's ability to provide immediate, continual, or exclusive access to the facilities; it will probably limit the liability of the service firm to specific and direct damages arising from use of the facility provided.[96] Usually, the subscriber will be required to indemnify the service firm against third party claims arising from use of the facilities provided.[97]

II. STATUTORY REQUIREMENTS

Selected provisions of federal and state statutes address matters involving preparation for computer disaster recovery. Failure to meet the disaster recovery planning requirements of these provisions may give rise to criminal or civil liability.[98] In addition, courts may consider the standards set by these laws in formulating a common law theory of negligence.[99]

A. *Corporations Generally*

Foreign Corrupt Practices Act — Corporations are heavily regulated entities, particularly at the federal level. As discussed above, corporations are highly dependent on computers and electronic records, and these records are highly vulnerable to destruction in a disaster. Yet, no federal law appears to address this issue directly. The federal law that appears most applicable to computer disaster recovery for corporations generally was actually enacted for a very different purpose.

Commentators discussing computer disaster recovery generally agree that section 13 (b)(2) of the Foreign Corrupt Practices Act of 1977 (FCPA) may be read to require executives of public companies to take reasonable precautions to preserve computer records from

93. *Id. See also* Raysman & Brown, *Disaster Recovery Services Agreements*, N.Y.L.J., May 14, 1987, at 1, col. 1.

94. *See* Raysman & Brown, *supra* note 93, at 30, col. 3.

95. *Id.* at 30, col. 2.

96. *Id. See also* Ainsworth, *supra* note 40, at 57, col. 4.

97. *See* Raysman & Brown, *supra* note 93, at 30, col. 2.

98. *See infra* notes 111 and 157 and accompanying text.

99. *See infra* notes 206-210 and accompanying text.

destruction.[100] The FCPA was originally intended to curb foreign bribery, safeguard corporate assets,[101] and so protect the reliance of investors.[102] To accomplish its purpose, the FCPA requires that corporations establish procedures to preserve accurate records and allow reliable auditing.[103] The language of this provision, however, may be interpreted to give the Act enormous scope.[104] The FCPA's internal audit and control requirements could conceivably extend into every aspect of corporate operations, leading some commentators to wonder if it provides the basis for a federal law of corporations.[105] The language of the statute would likely extend to require proper control and safeguards for a corporation's immensely valuable electronic data processing assets.[106]

Courts that have thus far interpreted this statute's language have already indicated that its requirements apply not only to written documents, but to the preservation of accurate computer records as well.[107] For example, in *S.E.C. v. World-Wide Coin In-*

---

100. *See* Sherman, *supra* note 32, at 51; West, *supra* note 6, at 62; Whitehead & Conyers, *supra* note 32, at 9.

101. *See* Siedel, *Internal Accounting Controls Under the Foreign Corrupt Practices Act: A Federal Law of Corporations?*, 18 AM. BUS. L.J. 443, 463, 473 (1981).

102. SEC v. World Wide Coin Investments, Ltd., 567 F. Supp. 724, 746 (N.D. Ga. 1983); Lewis v. Sporck, 612 F. Supp. 1316, 1333 (D. Cal. 1985).

103. 15 USC § 78m(b)(2) (1982) reads in pertinent part:

(2) Every issuer which has a class of securities registered pursuant to section 781 of this title and every issuer which is required to file reports pursuant to section 780(d) of this title shall —

(A) make and keep books, records, and accounts, which, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the issuer; and

(B) devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that —

(i) transactions are executed in accordance with management's general or specific authorization;

(ii) transactions are recorded as necessary (I) to permit preparation of financial statements in conformity with generally accepted accounting principles or any other criteria applicable to such statements, and (II) to maintain accountability for assets;

(iii) access to assets is permitted only in accordance with management's general or specific authorization; and

(iv) the recorded accountability for assets is compared with existing assets at reasonable intervals and appropriate action is taken with respect to any differences.

104. Siedel, *supra* note 101, at 444.

105. *Id.*

106. Guidelines issued by other federal agencies have already explicitly recognized computer disaster recovery planning as a necessary extension of a firm's internal control and physical security. *See infra* notes 127 and 131 and accompanying text.

107. World Wide Coin Investments, Ltd., 567 F. Supp. at 749; *see also* ABA Committee on Corporate Law, *A Guide to the New Section 13(b)(2) Accounting Requirements of the FCPA*, 34 BUS. LAW., 301, 324 (1978) [hereinafter *Guide*] (standards evolving to include data processing).

vestments, Ltd. the court interpreted the FCPA to require "reasonable" assurances of accuracy.[108] The court defined "reasonable" on the basis of economic cost/benefit analysis: implementation of the required procedures was not to create a fail safe system at all costs; rather, the costs should not exceed the expected benefits.[109] This sort of evaluation suggests that factors of computer record vulnerability should be weighed in the manner discussed above for evaluating a firm's disaster recovery needs.[110] Presumably, then, some corporations will need no more than frequent file backup; others may require alternate computer facilities to meet the statute's requirements.

Corporate executives who fail to determine the proper measure of disaster recovery preparation could become subject to certain criminal penalties. The Securities Exchange Commission, in enforcing this statute, may seek injunction against noncompliance, institute administrative proceedings, or even institute criminal proceedings.[111] The FCPA requires willful or knowing violation of its provisions before liability attaches.[112] Under the latter standard, however, corporate officers and directors need not intend to violate the statute in order to be guilty of violating its requirements; no scienter is required.[113] The FCPA does not provide for civil penalties, however; courts have held that the statute creates no private cause of action for injured parties such as investors, shareholders, or customers.[114]

SEC regulations — Certain other regulations enforced by the Securities Exchange Commission suggest the need for particular institutions to prepare an adequate disaster recovery plan. Investment companies and investment advisers are required by federal law to maintain accurate records of their transactions.[115] The SEC has recently approved storage of such records on computer media, subject to certain restrictions.[116] Both types of firms must maintain

108. World Wide Coin Investments, Ltd., 567 F. Supp. at 751; *see also Guide, supra* note 107, at 319.

109. World Wide Coin Investments, Ltd., 567 F. Supp. at 751.

110. *See supra notes* 24-26 and accompanying text.

111. *See Guide, supra* note 107, at 318-19.

112. 15 USC § 78m(a) (1982).

113. 15 USC § 78m(b)(2)(B) (1982); *see also* World Wide Coin Investments, Ltd., 567 F. Supp., at 749 (scienter not required).

114. Sporck, 612 F. Supp. at 1332.

115. 17 C.F.R. §§ 270.31a-2, 275.204-2 (1988).

116. 17 C.F.R. §§ 270.31a-2(f), 275.204-2(g); *see also Investment Companies May Keep Records on Microfilm, Computer Tapes,* 17 SEC. REG. L. REP. (BNA) 64 (1985); *SEC Proposes Allowing Mutual Funds to Keep Records on Magnetic Disk, Tapes,* 18 SEC. REG. L. REP. (BNA) 942 (1986).

separate back-up records, although these need not necessarily be stored off-site.[117] The details of storing and updating the duplicate records are left to the firms' determination.[118] Investment advisers must make "adequate provisions" to promptly furnish SEC examiners with such records.[119] The records must be made available within twenty-four hours, except in unusual circumstances.[120] Both types of firm must "reasonably safeguard" and be "ready at all times" to provide the required records.[121]

These regulations clearly require investment and investment adviser firms to create backup records — a disaster preventive measure. Requiring the records to be promptly available suggests the necessity of disaster recovery measures; while a computer disaster is certainly an "unusual circumstance," such an event could make the required records unavailable for weeks.[122] However, these regulations, much like the requirements of the FCPA, place on the affected corporations the burden of determining what preventive or recovery measures are necessary. The measures employed must again be "reasonable," suggesting that the same sort of cost/benefit analysis necessary under the FCPA will be necessary here.[123]

B. *Banks and Financial Institutions*

Federal regulatory agencies — Banks and similar financial institutions have received particular attention in the matter of computer disaster recovery, perhaps because of the fiduciary or trustee role they perform. In 1983, the Comptroller of the Currency first recognized the dependence of the banking industry on electronic data processing, and urged the development of contingency plans in case of emergency.[124] Since that time, the Office of the Comptroller (OCC) has issued several bulletins on computer disaster recov-

117. 17 C.F.R. §§ 270.31a-2(f)(iii), 275.204-2(g)(iii); Amendment to Investment Adviser Recordkeeping Rule, [1984-85 Transfer Binder] FED. SEC. L. REP. (CCH) ¶ 83,727 at 87,273 (Jan. 23, 1985) [hereinafter Amendment]; Adoption of an Amendment to an Investment Company Act Recordkeeping Rule [1986-87 Transfer Binder] FED. SEC. L. REP. (CCH) ¶ 84,042A (Nov. 26, 1986) [hereinafter Adoption].

118. Adoption, *supra* note 117; Amendment, *supra* note 117.

119. Amendment, *supra* note 117 at 87, 274.

120. *Id.*

121. 17 C.F.R. §§ 270.31a-2(f)(ii),(iv), 275.204-2 (g)(ii), (iv).

122. *See e.g., supra* note 65 and accompanying text.

123. *See supra* notes 107-110 and accompanying text.

124. *See generally* Mitchell, *Protecting Banks Against Failure of Data Processing*, N.Y.L.J., April 22, 1987, at 1, col. 1; Sherizen & Belisle, *Begin Contingency Planning or You Might Become an Outlaw*, COMPUTERWORLD SPOTLIGHT No. 48, July 11, 1988, at S-10, col. 2.

ery.[125] These bulletins recommend development of alternate data processing capability for national banks, including off-site backup of important files, critical software, and computer hardware.[126] The most recent bulletin recognizes computer disaster recovery as a necessary extension of a bank's internal control and physical security.[127] Where banks are dependent on outside data processing, such as a service bureau, the bank should review that vendor's contingency plans.[128] The OCC has also stated its policy of holding a bank's board of directors responsible for an annual review of these disaster recovery plans.[129] The OCC bulletins require that a bank's plan be "testable", which seems to effectively preclude the use of cold sites.[130]

In addition to the OCC bulletins, the Federal Home Loan Bank Board (FHLBB) has issued a memorandum requiring insured institutions to develop disaster recovery plans.[131] This memorandum also recognizes disaster recovery plans as "an extension of internal control and physical security" measures. The memorandum labels reciprocity agreements "not sufficient" as preparation for the needs of savings institutions in a disaster, because of objections to this option discussed above.[132] Thus, in weighing disaster recovery considerations, at least two planning options appear foreclosed to executives of regulated savings institutions.[133]

Uniform Commercial Code — The Uniform Commercial Code (UCC) governs commercial transactions; it has been enacted in whole or in part by every state legislature.[134] Section 4 of the UCC limits the amount of time a bank has available to return a dishonored check.[135] The bank is required to exercise ordinary care

125. Comptroller of the Currency, Administrator of National Banks, Banking Circular BC-177 (April 16, 1987). *See also* Koselka, *supra* note 1, at 80; Mitchell, *supra* note 124; Stamps, *supra* note 21, at 63.

126. *See* Mitchell, *supra* note 124, at 6, col. 3.

127. Banking Circular BC-177, *supra* note 125, at 1.

128. *Id.* The OCC has taken action against at least one service that offered outside data processing to banks, charging that the service's computer disaster recovery plans were inadequate. *Cease and Desist Order Entered Against National Bank EDP Provider*, [1984-84 Transfer Binder] FED. BANKING L. REP. (CCH) ¶ 86,238 (Oct. 10, 1985).

129. *Id. See also* Koselka, *supra* note 1, at 80; Stamps, *supra* note 21, at 63.

130. *See* Koselka, *supra* note 1, at 80.

131. Federal Home Loan Bank Board, Office of Examinations and Supervision, Memorandum R-67 (Sept. 4, 1986). *See also* Melia, *supra* note 13, at S-72; Regulations, *supra* note 61, at 115.

132. Memorandum R-67, *supra* note 131.

133. *See supra* notes 24-26 and accompanying text.

134. UNIFORM COMMERCIAL CODE §§ 4-101 to 8-406, U.L.A., at iii (1977).

135. *See* U.C.C. §§ 4-301, 4-302(5) (1977).

in determining whether to dishonor and return a check.[136] Failure to return a dishonored check within the prescribed time limit, the so-called "midnight deadline," leaves the bank liable for the amount of the check, less the sum unrecoverable even had ordinary care been exercised in collection.[137] U.C.C. § 4-108 permits a bank to exceed the midnight deadline if its normal operations are disrupted by natural disasters or certain other circumstances beyond the bank's control.[138] The bank must take "reasonable" measures and "exercise such diligence as the circumstances require" to prepare for such circumstances.[139] Comment 4 to this section states that only this measure of diligence in the face of a disaster such as an "act of God" excuses the bank from liability.[140]

Courts interpreting this provision have considered the question of equipment failure as an unforeseeable circumstance beyond the bank's control. In *Blake v. Woodford Bank & Trust Co.*, a bank was unable to return a dishonored check before the midnight deadline because of mechanical equipment failure and an unusually heavy workload.[141] The court found, however, that a heavy workload over the Christmas holidays was foreseeable; in addition, the machinery in question had broken down before.[142] The court found the bank liable because it could reasonably have taken steps to avoid the delay.[143]

This standard has been applied to cases of computer breakdown. The Montana Supreme Court considered a case in which a bank failed to return a dishonored check in time due to circum-

---

136. *See* U.C.C. § 4-103(3) (1977).

137. *See* U.C.C. §§ 4-104(1)(h), 4-103(5) (1977).

138. U.C.C. § 4-108(2) (1977).

139. U.C.C. § 4-108 reads in pertinent part:

(2) Delay by a collecting bank or payor bank beyond time limits prescribed or permitted by this act or by instructions is excused if caused by interruption of communication facilities, suspension of payments by another bank, war, emergency conditions or other circumstances beyond the control of the bank provided it exercises such diligence as the circumstances require.

140. The Official Comment to this section states, in pertinent part:

This section operates, however, only in the types of situation specified. Examples of these situations include blizzards, floods, or hurricanes, and other "Act of God" events or conditions, and wrecks or disasters . . . . When delay is sought to be excused under this subsection the bank must "Exercise such diligence as the circumstances require" and it has the burden of proof. U.C.C. § 4-108(2), comment 4 (1977).

141. Blake v. Woodford Bank & Trust Co., 555 S.W.2d 589 (Ky. Ct. App. 1977). *See also* Brown, *Some Current Litigation Issues Arising from the Use of Computer Systems in the Rendering of Financial Services*, COMPUTER L. & PRAC., Mar./Apr. 1988, at 119.

142. *Id.* at 596.

143. *Id.*

stances including a flood and computer malfunction.[144] The court found the bank liable in that instance, because the relationship between the parties was extraordinary, requiring more than ordinary care.[145] Presumably, had the relationship required only ordinary care, the bank would have been excused from liability. However, a computer breakdown of twenty-four hours has been held not to justify a check processing delay of four days.[146] One court has gone so far as to rule that the inability of a bank to process a check by computer does not constitute sufficient emergency to excuse the bank from returning a dishonored check in a timely fashion; the court implied that, in the absence of functional computer equipment, the bank should perhaps have processed the checks by hand![147]

Planning and implementation of computer disaster recovery measures appear to help a bank meet the necessary standard of care to avoid liability in these cases. In *Port City State Bank v. American Nat'l Bank*, a bank failed to return a check within the prescribed U.C.C. time limits because of computer equipment failure, but was relieved of liability under § 4-108.[148] In that case, the bank had previously entered a reciprocity agreement with another firm; upon failure of its own equipment, the bank implemented measures to transfer its electronic data processing functions to the backup site.[149] The bank also implemented measures to repair its own equipment.[150] The court found the computer breakdown to be a circumstance beyond the bank's control;[151] it also found that the bank had exercised due diligence both in its attempts to repair the computer,[152] and in its implementation of the disaster recovery plan.[153] In a more recent case, a New York court found a bank liable for not developing some computer disaster recovery plan before a foreseeable computer breakdown.[154] The court stated that

144. Sun River Cattle Co, Inc. v. Miners Bank, 164 Mont. 287, 521 P.2d 679 (1974); *see also* First Wyo. Bank, N.A. v. Cabinet Craft Distrib., Inc., 624 P.2d 227 (Wyo. 1981).

145. Sun River, 521 P.2d at 689.

146. N.C. Nat'l Bank v. S.C. Nat'l Bank, 449 F. Supp. 616 (D.S.C. 1976), *aff'd*, 573 F.2d 1305 (4th Cir. 1978).

147. Bank Leumi Trust Co. v. Bank of Mid-Jersey, 499 F. Supp. 1022, 1025 (D.N.J. 1980), *aff'd*, 659 F.2d 1065 (3rd Cir. 1981).

148. Port City State Bank v. Am. Nat'l Bank, 486 F.2d 196 (10th Cir. 1973).

149. *Id.* at 198.

150. *Id.*

151. *Id.* at 200.

152. *Id.*

153. *Id.*

154. Congress Factors Corp. v. Extebank, 32 U.C.C. Rep. Serv. (Callaghan) 1559, 1560 (N.Y. Civ. Ct. 1982).

the bank in question had not exercised due diligence when it failed to develop alternate check processing systems in light of previous computer failures.[155]

While these cases do not deal specifically with preparations for data processing systems recovery in a natural disaster, they do discuss the question of liability for computer malfunction. In defining reasonable precautions under the UCC, these decisions employ standards of foreseeability and ordinary care derived from tort law. However, damages recoverable under these statutes are severely circumscribed; where losses are limited to the face value of a dishonored check, there is little potential for serious economic harm.

Electronic Funds Transfer Act — The Electronic Funds Transfer Act (EFTA) was designed to protect consumers from at least some of the financial losses that could result from increased dependence on electronic data processing.[156] Among its other safeguards, the act makes banks liable for actual damages proximately caused by failing to transfer the correct sum of money in a timely fashion.[157] As under UCC section 4, though, the bank is excused from liability where the transfer is disrupted by an "act of God," that is, some disaster beyond the bank's control.[158] The bank must have taken reasonable precautions against such an event.[159] While no reported case has yet interpreted this provision of the act, the language and nature of the statute indicate that the standard for "reasonable" should closely parallel the term's meaning under the language of U.C.C. § 4-108(b). This standard of reasonable precautions will certainly take into account provisions made for disaster recovery.[160]

Unlike the UCC, the EFTA authorizes recovery of all damages

---

155. *Id.* at 1560.

156. *See generally* Broadman, *Electronic Fund Transfer Act: Is the Consumer Protected?*, 13 U.S.F. L. REV. 245, 260-61 (1979); Budnitz, *Problems of Proof When There's a Computer Goof: Consumers v. ATM's*, 2 COMPUTER L.J. 49, 73 (1980); Katskee & Wright, *An Overview of the Legal Issues Confronting the Establishment of Electronic Funds Transfer Services*, 2 COMPUTER L.J. 7, 21 (1980).

157. 15 U.S.C. § 1693h(a)(1) (1982).

158. 15 U.S.C. § 1693h(b) reads in pertinent part: ACTS OF GOD AND TECHNICAL MALFUNCTIONS

(b) A financial institution shall not be liable under subsection (a)(1) or (2) of this section if the financial institution shows by a preponderance of the evidence that its action or failure to act resulted from —

(1) an act of God or other circumstance beyond its control, that it exercised reasonable care to prevent such an occurrence, and that it exercised such diligence as the circumstances required . . .

159. 15 U.S.C. § 1693h(b)(1) (1982).

160. *See* Broadman, *supra* note 156, at 260-61.

proximately caused by the bank's failure.[161] The magnitude of possible harm in electronic funds transfer is perhaps greater than that in handling checks. However, the EFTA applies only to consumer transactions; no similar provision has been made for commercial electronic funds transfers.[162] Such transactions fall outside the scope of both the UCC and EFTA; they are governed by principles of contract law.[163] Commercial firms relying on electronic funds transfer must therefore contractually distribute any liability for losses among themselves. The consumer who relies on electronic funds transfer is not in a strong bargaining position, and so is protected under the EFTA.[164] Part III examines how courts have distributed corporate liability in the absence of such statutory provisions.

III. COMMON LAW NEGLIGENCE

While courts have not directly addressed the question of computer disaster preparation, several broad rules of duty and liability for corporations and their agents are firmly established. The doctrines are fairly uniform, with some minor variation between jurisdictions. Many states have codified these doctrines; occasionally they may be modified by local statutory provisions.[165] These rules may be applied to the specific question at hand, forming the basis for a particular theory of tort liability for losses in data processing disasters.

A. *Liability of Corporations*

Corporations, as legal entities, are generally liable for negligent acts just the same as other individuals.[166] Corporations, however, can only act through their officers, directors, or agents.[167] Corporations may be held liable for the negligent acts of their agents if the

161. 15 U.S.C. § 1693h(a) (1982).

162. 15 U.S.C. § 1693h (1982).

163. *See* Evra Corp. v. Swiss Bank Corp., 673 F.2d 951, 955 (1982).

164. *See* Katskee & Wright, *supra* note 156.

165. *See* Special Project, *An Historical Perspective on the Duty of Care, the Duty of Loyalty, and the Business Judgment Rule*, 40 VAND. L. REV. 605, 608 n.15 (1987) (authored by Marcia M. McMurray).

166. *See e.g.*, Garcia v. San Gabriel Ready Mixt, 155 Cal. App. 2d 568, 572, 318 P.2d 145, 148 (1957); Grow Farms Corp. v. Nat'l State Bank, 167 N.J. Super. 102, 400 A.2d 535, 538 (1979); Garafano v. Neshobe Beach Club, Inc., 126 Vt. 566, 569, 238 A.2d 70, 73 (1967).

167. *See e.g.*, Fort Worth Elevator Co. v. Russel, 123 Tex. 128, 70 S.W.2d 397 (Tex. Ct. App. 1934); O'Shea v. Pac. Gas & Elec., 18 Cal. App. 2d 32, 39, 62 P.2d 1066, 1070 (Cal. Ct. App. 1936).

agent is acting within the scope of his corporate responsibilities;[168] often, both the agent and the corporation will be liable for such acts.[169] Where the corporation owes a third party a duty, and the corporate agent fails to perform that duty, the injured party may recover for the omission.[170] Recovery, however, has been traditionally awarded only for physical damages; awards for pecuniary losses are usually granted only where the corporation is acting as a fiduciary or trustee.[171] Presumably, then, under the traditional common law standard, a corporation might be found liable for failure to provide computer recovery measures where the person or property of an outside party was physically damaged by the failure to act. This standard would define a rather narrow range of liability to outside parties. As discussed in Part IV, certain policy considerations indicate that this standard should be broadened for computer disaster recovery.[172]

B. *Liability of Corporate Executives*

Liability to the corporation — Under the common law, the legal responsibilities of a corporation's directors and officers include a fiduciary duty to the corporation.[173] These executives must therefore exercise due care to safeguard corporate assets;[174] this responsibility includes a duty to see that clear and accurate records are kept to prevent fraud.[175] Officers and directors who neglect their fiduciary duty to the corporation become liable to the corporation or to the shareholders for the losses incurred.[176]

---

168. *See e.g.*, Crittendon v. State Oil Co., 78 Ill. App. 2d 112, 222 N.E.2d 561 (1966).

169. *See e.g.*, Dunbar v. Demaree, 2 N.E.2d 1003, 1009 (Ind. App. 1936); O'Shea, 62 P.2d at 1070.

170. *In re* Sabbatino & Co., 150 F.2d 101 (2nd Cir. 1945). *See e.g.*, Mortimer v. Farmers' Mutual Fire and Lighting Ins. Ass'n, 249 N.W. 405, 407 (Iowa 1933); Electric Supply Co. v. Rosser, 214 P. 1068 (1923).

171. *See* Mortimer, 249 N.W. at 407.

172. *See infra* notes 226-230 and accompanying text.

173. *See e.g.*, *In re* Adams Lab, 3 Bankr. 495 (Bankr. E.D. Va. 1980); Smith v. Van Gorkom, 488 A.2d 858, 873 (Del. 1985); Professional Hockey Corp. v. World Hockey Ass'n, 143 Cal. App. 3d 410, 191 Cal. Rptr. 773, 776 (Cal. Ct. App. 1983); Bayer v. Beran, 49 N.Y.S. 2d 2, 5 (N.Y. Sup. Ct. 1944); *see also* H. HENN & J. ALEXANDER, LAWS OF CORPORATIONS 627 (3rd ed. 1983).

174. *See e.g.*, Atlantic Accoustical & Insulation Co. v. Moreira, 348 A.2d 263 (Me. 1975); *see generally* Special Project, *supra* note 165, at 607.

175. *See e.g.*, Backus v. Finkelstein, 23 F.2d 357, 364 (D. Minn. 1927); Hollander v. Breeze Corp., 131 N.J. Eq. 585, 26 A.2d 507, 519 (N.J. Ch. 1941), *aff'd*, 131 N.J. Eq. 613, 26 A.2d 522 (N.J. 1942).

176. *See e.g.*, Sternberg v. Blaine, 179 Ark. 448, 449, 17 S.W.2d 286, 288 (1929); Magale v. Fomby, 132 Ark. 289, 201 S.W. 278 (1918); Medford Trust Co. v. McKnight, 292 Mass. 1, 197 N.E. 649 (1935); *see also* H. HENN & J. ALEXANDER, *supra* note 173, at 624.

In managing the affairs of a corporation, the directors and officers are held to a standard of ordinary care.[177] Courts in different jurisdictions have defined this standard in two different ways; one definition describes a more objective standard, the other a more subjective standard.[178] In some jurisdictions, courts have found that ordinary care means the care that would be exercised by a prudent person in the same circumstances.[179] Other courts hold ordinary care to mean the care the executives in question would exercise in managing their own affairs.[180]

Under either definition, officers and directors are not insurers of corporate assets, and are not liable for errors made in good faith.[181] Courts have widely applied this "good faith" standard in the form of the business judgment rule.[182] Corporate executives are not liable to the corporation for losses where they have made an informed business judgment.[183] The business judgment rule applies except in cases where fraud or gross negligence on the part of the executives is shown.[184] The business judgment rule is also limited to cases of an actual judgment; failure to make an informed business judgment has been held to constitute gross negligence.[185] Thus, inaction by officers and directors does not fall within the purview of

177. *See e.g.*, Bourne v. Perkins, 42 F.2d 94, 99 (8th Cir. 1930); Chicago Title & Trust Co. Munday, 297 Ill. 555, 131 N.E. 103 (Sup. Ct. Ill. 1921); Prudential Trust Co. v. Brown, 271 Mass. 132, 171 N.E. 42 (1930); Casey v. Woodruff 49 N.Y.S.2d 625, 643 (N.Y. App. Div. 1944); Williams v. Fidelity Loan, 142 Va. 43, 128 S.E. 615 (1925).

178. *See generally* Comment, *Director Liability Under the Business Judgment Rule: Fact or Fiction?*, 35 SW. L.J. 775 (1981) (authored by Michele H. Ubelaker).

179. *See e.g.*, Weidner v. Engelhart, 176 N.W.2d 509, 518 (N.D. 1970); *see also generally* Comment, *supra* note 178, at 787; H. HENN & J. ALEXANDER, *supra* note 178, at 622-23.

180. *See e.g.*, Ashby v. Peters, 128 Neb. 338, 258 N.W. 639, 99 A.L.R. 843 (1953); Simon v Socony Vacuum Oil Co., 179 Misc. 202, 203, 38 N.Y.S.2d 270, 273 (N.Y. Sup. Ct. 1942), aff'd, 267 A.D. 890, 47 N.Y.S.2d 589 (1944); *see also generally* Comment, *supra* note 178, at 787.

181. *See e.g.*, Abbey v. Control Data Corp., 603 F.2d 724 (8th Cir. 1979); Weidner, 176 N.W.2d 509; Prudential Trust Co., 171 N.E. 142; Simon, 179 Misc. at 203, 38 N.Y.S.2d at 273; Bayer, 49 N.Y.S.2d at 5-6; *see also generally* Comment, *supra* note 178, at 792.

182. *See e.g.*, Gearhart v. Smith Intern, Inc., 741 F.2d 707, 719 (5th Cir. 1984); Kelley v. Bell, 266 A.2d 878 (Del. 1970); Bayer, 49 N.Y.S.2d at 6; *see also generally* Special Project, *supra* note 165, at 613; Comment, *supra* note 178.

183. *See e.g.*, Van Gorkom, 488 A.2d at 879; Eldridge v. Tymshare, Inc., 186 Cal. App. 3d 767, 776, 230 Cal. Rptr. 815, 820 (Cal. Ct. App. 1986); *see also* H. HENN & J. ALEXANDER, *supra* note 173, at 661.

184. *See e.g.*, Jardel Co. v. Hughes, 523 A.2d 518, 530 (Del. 1987); Rettinger v. Pierpont, 145 Neb. 161, 15 N.W.2d 393, 412 (1944); *see also* Lewis v. Anderson 615 F.2d 778, 781-82 (9th Cir. 1979).

185. *See e.g.*, Van Gorkom, 488 A.2d at 872; *see also* H. HENN & J. ALEXANDER, *supra* note 173, at 625.

this rule.[186]

Officers and directors of a corporation are therefore liable for the consequences of their failure to act.[187] Failure to exercise reasonable supervision and be informed of corporate affairs constitutes negligence.[188] Ignorance or want of knowledge carries the same liability for corporate officers and directors as does failure to act.[189] Specific losses due to inattention are actionable as a tort of omission;[190] directors and officers are responsible for those losses due to omission.[191] Presumably, then, officers and directors of a corporation would be liable under the common law standard for failure to consider and make an informed business judgment concerning their firm's computer disaster recovery options.

Liability to outside parties — Generally, the officers and directors of a corporation will not be personally liable for injuries to third parties if their actions were undertaken in their capacities as corporate executives.[192] However, this rule has certain notable exceptions. These corporate executives become personally liable if they directed or participated in the tort.[193] Officers and directors are also liable for their failure to act where they owe a duty to the outside party, and not merely to the corporation.[194] Duties that are owed to a third party rather than to the corporation fall outside the

186. *See e.g.*, Casey, 49 N.Y.S.2d 625; *see also* Burt v. Irvine Co., 237 Cal. App. 2d 828, 852, 47 Cal. Rptr. 392, 401-408 (1965).

187. *See e.g.*, Frances T. v. Village Green Owners Ass'n, 42 Cal. 3d 490, 505, 229 Cal. Rptr. 456, 464, 723 P.2d 573, 580 (1986); Chicago Title & Trust Co., 297 Ill. 555, 131 N.E. 103; *see also* H. HENN & J. ALEXANDER, *supra* note 173, at 621; Fisher v. Parr, 92 Md. 245, 48 A. 621 (1901); Olin Matheson Chem. Corp. v. Planters Corp., 236 S.C. 318, 326, 114 S.E.2d 321 (1960).

188. *See e.g.*, Francis v. United Jersey Bank, 87 N.J. 15, 432 A.2d 814, 821 (1981); Olin v. Matheson, 114 S.E.2d 321; Casey, 49 N.Y.S.2d 625; *see also* Hornsby v. Internal Revenue Serv., 588 F.2d 952, 953 (5th Cir. 1979).

189. *See e.g.*, Prudential Trust Co., 171 N.E. 42, 44; Ashby v. Peters, 128 Neb. 338, 258 N.W. 639, 644 (1939); *see also* Bowerman v. Hamner, 250 U.S. 504, 511 (1919).

190. *See e.g.*, Barnes v. Andrews, 298 F. 614, 616 (S.D.N.Y. 1924).

191. *See e.g.*, Fisher, 92 Md. 245, 48 A. 621; *see also* Medford Trust Co. v. McKnight, 197 N.E. 649, 655 (Mass. 1935); Magale, 132 Ark. 289, 201 S.W. 278.

192. *See e.g.*, *In re* Knight, 60 Ill. App. 2d 457, 460, 208 N.E.2d 679, 681 (Ill. 1965); Michaels v. Lispenard Holding Corp., 201 N.Y.S.2d 611, 614, 11 A.D.2d 12, 14, (N.Y. App. Div. 1960); *see also* H. HENN & J. ALEXANDER, *supra* note 173 at 625; RESTATEMENT (SECOND) OF AGENCY § 352 (1958).

193. *See e.g.*, Levi v. Schwartz, 201 Md. 575, 95 A. 2d 322, 36 A.L.R. 2d 1241 (1953); Sternberg, 17 S.W.2d at 288; United States Liability Ins. Co. v. Haidinger-Hayes, Inc., 1 Cal. 3d 586, 595, 83 Cal. Rptr. 418, 423, 463 P.2d 770, 775 (1970).

194. *See e.g.*, Haidinger-Hayes, Inc., 1 Cal. 3d at 586, 83 Cal. Rptr. at 423, 463 P.2d at 775; Frances T., 723 P.2d at 582; Adams v. Fiduciary Casualty Co., 107 So. 496, 502 (La. Ct. App. 1958); Michaels, 201 N.Y.S.2d at 614, 11 A.D.2d at 14; *see also* RESTATEMENT (SECOND) OF AGENCY § 354 comment a (1958).

protection of the business judgment rule.[195] Such a duty is generally found when the corporation in question is a bank or similar institution that holds funds in trust;[196] the executives of such institutions have been held to owe a fiduciary duty directly to the depositors.[197] Occasionally, this duty may be owed to creditors, especially where the bank has become insolvent.[198] In rare instances a corporation other than a bank or trust may owe creditors such a duty.[199] Where the duty exists, though, recovery from each executive depends upon proving that particular executive personally negligent.[200] In addition, damages for purely pecuniary losses have traditionally not been awarded unless the corporation in question is a bank.[201] Thus, like the corporation itself,[202] corporate officers and directors who fail to take adequate computer disaster recovery measures would be liable to outside parties only for physical damages where the executives directly owed the third party a duty of care. In Part IV, we examine the implications and adequacy of this standard in light of the purposes of tort law.

IV. A THEORY OF LIABILITY

As described above, the liability of negligent corporations and their executives has traditionally been fairly limited. Yet, as discussed in the Introduction to this paper, negligence in computer disaster recovery may create enormous losses to corporations, third parties, and society in general. The statutes and regulations discussed in Part II fail to address this problem outside of certain specific instances. However, doctrines of tort law provide a basis for addressing the problem through the common law.

A. *Standards of Negligence*

Statutory Standards — In our increasingly complex society, different interests are bound to collide; tort law exists to compensate

195. *See e.g.*, Frances T., 723 P.2d at 584.

196. *See e.g.*, Francis, 432 A.2d at 824.

197. *See id.* at 824; *but see* Chester-Cambridge Bank & Trust Co. v. Rhodes, 346 Pa. 427, 432, 31 A.2d 128, 131 (1943).

198. *See e.g.*, Francis, 432 A.2d at 824; Sternberg, 17 S.W.2d at 288; *but see* Allen v. Cochran, 160 La. 425, 107 So. 292 (1926); Chester-Cambridge, 363 Pa. 427, 432, 31 A.2d 128, 131 (1943).

199. *See e.g.*, Veeser v. Robinson Hotel Co., 275 Mich. 133, 266 N.W. 54 (1936).

200. *See e.g.*, Levi, 201 Md. 575; Frances T., 723 P.2d 573.

201. *See e.g.*, Haidinger-Hayes, Inc., 1 Cal. 3d at 586, 83 Cal. Rptr. at 423, 463 P.2d at 775; *see also* RESTATEMENT (SECOND) OF AGENCY § 357 (1958).

202. *See supra* notes 166-172 and accompanying text.

those whose interests are unfairly injured is such clashes.[203] Courts are often called upon to fashion novel remedies to compensate those injured in novel situations.[204] In fashioning such remedies, courts must determine which injuries deserve compensation; in tort law, this is generally determined by finding a societally acceptable duty of care which an offending party may have breached to cause another injury.[205] Courts often find an applicable duty of care in the standard set by legislative enactments or administrative regulation.[206] The statute or regulation adopted should be designed to protect a defined class of persons from the particular harm that has occurred.[207] Where such statutes or regulations provide for civil liability, the court awards the measure of damages prescribed.[208] Where civil liability is not provided for, the court may find civil liability to be implied in the statute's language.[209] Or, if civil liability is not implied, the court may simply adopt the legislative standard in fashioning a common law remedy.[210]

Courts have in this fashion found a duty for some institutions to preserve and make available certain records. In *Quinones v. United States*, a discharged employee claimed that his former employer had negligently lost or destroyed his personnel records, and so injured his future job prospects.[211] The court held that the employer had a duty to use reasonable care in maintaining personnel records; the court based this holding on the standard required by a federal administrative regulation.[212] Similarly, courts have found a hospital to have a duty to use reasonable care in keeping patients' medical records.[213] In *Fox v. Cohen*, a patient charged that a hospital had negligently lost or destroyed certain medical records, making it impossible to prove malpractice.[214] The *Fox* court found a

203. *See* Wright, *Introduction to the Law of Torts*, 8 CAMBRIDGE L.J. 238, 238 (1944).

204. *Id.*; W. PROSSER & W. KEETON, THE LAW OF TORTS § 1, at 3-4 (5th ed. 1984). For recent examples of such developments, *see infra* notes 214 and 238-247.

205. W. PROSSER & W. KEETON, *supra* note 204, at 4.

206. RESTATEMENT (SECOND) OF TORTS §§ 285-286 (1958).

207. *Id.*

208. *Id.* at § 285 comment b.

209. *Id.* at § 286 comment d.

210. *Id.* at § 285 comment c; *see also* Frederick L. v. Thomas, 578 F.2d 513 n. 8 (3rd Cir. 1978) (though closely related, negligence *per se* is distinct from implied civil liability).

211. Quinones v. United States, 492 F.2d 1269 (3rd Cir. 1974).

212. Quinones, 492 F.2d at 1277. *See also* Bulkin v. Western Kraft East Inc., 422 F. Supp. 437, 443 (E.D. Penn. 1976) (following *Quinones*).

213. Fox v. Cohen, 84 Ill. App. 3d 744, 406 N.E.2d 178 (Ill. App. Ct. 1980); Bondu v. Gurvich (Fla. App. 1984).

214. Fox, 406 N.E.2d at 182. Some courts have extended this approach to create a new tort for spoilation of evidence. *See* Petrik v. Monarch Printing Corp., 150 Ill. App. 3d 248,

duty on the hospital's part to use reasonable care in maintaining records; this duty was based on the standard set by administrative regulations and hospital association standards.[215]

Through similar reasoning, the statutes and administrative regulations explored in Part II may provide the standard for maintenance and accessibility of computer records. Quite apart from their own penalties or requirements, such statutes and regulations define acceptable standards for common law tort actions. The statutes make adequate disaster recovery provisions an integral part of reasonable care in preserving and maintaining computer records.[216] Some statutes, such as the EFTA or UCC provisions, provide for civil actions;[217] where such a statute sets the applicable standard, the court should adopt the measure of damages provided in the statute.[218] The FCPA, however, does not create a private cause of action.[219] Nonetheless, the FCPA protects a specific class of persons from a particular harm, and may properly be applied to tort suits.[220] Where such a statute sets the applicable standard the court is free to award whatever measure of damages will compensate the victim for his injury.[221]

If no statute sets an applicable standard, courts may look to similar statutes and regulations for guidance in fashioning a duty of care.[222] The decision making process discussed in Part I of this article constitutes a common thread in both the statutory and common law doctrines discussed in Parts II and III. In weighing the costs and benefits of computer disaster recovery for a firm, a corporate officer or director makes the sort of judgment protected under the business judgment rule.[223] Such consideration of corporate options, regardless of the actual conclusion, is the sort of deliberation necessary to ordinary care in managing corporate assets and protecting corporate records.[224] This standard closely parallels the statutory requirements for reasonable safeguards and due care inte-

---

501 N.E.2d 1312 (Ill. App. Ct. 1986); *see also generally* Comment, *Spoilation: Civil Liability for Destruction of Evidence*, 20 U. RICH. L. REV. 191 (1985) (authored by Andrea H. Rowse).

215. Fox, 406 N.E.2d at 182-83.

216. *See* sources cited *supra* notes 107, 121, 141, and 148.

217. *See* sources cited *supra* notes 136 and 161.

218. *See supra* note 208 and accompanying text.

219. *See supra* note 114 and accompanying text.

220. By similar application, statutes such as the National Bank Act have provided a standard for common law negligence actions. *See* Michelsen v. Penney 135 F.2d 409, 419 (2nd Cir. 1943); *see also supra* note 207 and accompanying text.

221. RESTATEMENT (SECOND) OF TORTS § 906 comment a (1965).

222. *See* sources cited *supra* note 210.

223. *See supra* notes 181-183 and accompanying text.

224. *See supra* notes 173-180 and accompanying text.

gral to the FCPA, federal administrative regulations, and section 4 of the UCC.[225]

Such considerations have long been an important element in assigning negligence liability. Judge Learned Hand, in the famous *Carroll Towing*[226] case, suggested that judges and juries, in determining negligence, should evaluate the probability of the particular harm occurring, the magnitude of the harm if it occurs, and the countervailing costs of prevention.[227] Judge Hand went so far as to reduce this formula to a mathematical representation, suggesting that where the product of the first two factors is greater than the third factor, the tortfeasor was negligent in not taking precautions.[228] Commentators such as Richard Posner have suggested that this formula defines a method for minimizing societal costs, making the label of "negligence" shorthand for a sort of legal cost/benefit analysis.[229] Assignment of liability on the basis of negligence thus serves to minimize societal costs by providing the proper measure of incentive to deter unacceptable future harm.[230]

Limiting factors — Negligence in tort law is often assigned on the basis of "foreseeability" and "notice."[231] These requirements act as limiting factors on the scope of the negligence standard, but weigh much the same considerations. Learned Hand's analysis cannot be applied where the probability and magnitude of harm are unforeseeable, and thus unmeasurable; thus a court may consider whether circumstances were such that the tortfeasor should have foreseen the possible harm in order to weigh it against the cost of prevention.[232] Similarly, the court may consider whether the tortfeasor was aware or should have been aware of the particular harm.[233] These considerations also imply a requirement to weigh the factors discussed in Part I[234], as illustrated by the application of the foreseeability standard in the UCC cases.[235]

---

225. *See supra* notes 148-154 and accompanying text.

226. United States v. Carroll Towing Co., 159 F.2d 169 (2nd Cir. 1947).

227. *Id.* at 173. *See also* Conway v. O'Brien, 111 F.2d 611 (2nd Cir. 1940).

228. Carroll Towing, 159 F.2d at 173.

229. Posner, *A Theory of Negligence*, 1 J. LEGAL STUD. 29, 32-33 (1972).

230. *See* W. PROSSER & W. KEETON, *supra* note 204, § 4, at 25-26.

231. *See e.g.*, Gordon v. Am. Museum of Natural History, 67 N.Y.2d 836, 492 N.E.2d 774 (1986); Negri v. Stop & Shop, Inc, 65 N.Y.2d 625, 480 N.E.2d 740 (1985); Trimarco v. Klein, 56 N.Y.2d 98, 436 N.E.2d 502 (1982).

232. *See* Evra Corp., 673 F.2d at 958 (Posner, J., discussing forseeability under Learned Hand analysis); *see also* RESTATEMENT (SECOND) OF TORTS §§ 291-293 (1965).

233. *See* RESTATEMENT (SECOND) OF TORTS § 290 (1965).

234. *See supra* notes 24-26 and accompanying text.

235. *See supra* notes 141-155 and accompanying text; *see also* Brown, *supra* note 141, at 122, n.7.

Courts may also limit the scope of negligence liability by requiring physical harm to the injured party or her property.[236] Traditionally, recovery of purely economic damages was determined by principles of contract law.[237] More recently, several courts have recognized the importance of compensating victims for pecuniary injuries; economic injury may be as damaging and as foreseeable as physical injury.[238] Developments in the law relating to negligent performance of professional services show the evolution of such a standard for third party recovery.[239] Accountants, lawyers, insurance adjusters, and other professionals were liable for negligent performance of their responsibilities only where privity of contract or a similar relationship existed.[240] More recently, courts in several jurisdictions have recognized that parties not in strict privity with these professionals may rely on their performance.[241] Thus, where a professional fails to meet the statutory or professional standards expected of her, she may be liable for economic harm to a third party if she should reasonably have expected that party to rely on her performance.[242]

This approach retains the limit of foreseeability, but allows compensation to third parties who are economically injured. Such a doctrine deserves consideration in fashioning a negligence standard for computer disaster recovery. As discussed above, third party liability of negligent corporations or executives has traditionally been severely circumscribed.[243] However, outside parties are often in a poor position to avoid losses when the electronic records maintained by a particular corporation become suddenly inaccessible.

---

236. *See* RESTATEMENT (SECOND) OF TORTS §§ 323, 324A (1965). *See also* sources cited *supra* notes 171 and 201.

237. *See* W. PROSSER & W. KEETON, *supra* note 204, § 92, at 657.

238. *See e.g.*, People's Express Airlines, Inc. v. Consol. Rail Corp., 100 N.J. 246, 495 A.2d 107 (1985) (tort compensation for purely economic harm).

239. *See e.g.*, Selden v. Burnett, 754 P.2d 256 (Alaska 1988) (criteria for negligent accountant's liability to third party) Continental Ins. Co. v. Bayless & Roberts, Inc., 608 P.2d 281 (Alaska 1980) (insurance adjuster found liable); First Am. Title Ins. Co. v. First Title Serv. Inc., 457 So.2d 467 (Fla. 1984) (title abstracter liable); AlumaKraft Mfg. Co. v. Elmer Fox & Co., 493 S.W.2d 378 (Mo. Ct. App. 1973) (accountant liable); Annotation, *What Constitutes Negligence Sufficient to Render Attorney Liable to Person Other than Immediate Client*, 61 A.L.R. 4th 464, § 2, at 473-78 (1988) (increased attorney liability). *See also* Rosenblum Inc. v. Adler, 93 N.J. 324, 329, 461 A.2d 138, 143 (1983) (negligent accountant found liable to third party).

240. *See* Ultramares Corp. v. Touche, 255 N.Y. 170, 189, 174 N.E. 441, 448 (1931); *see also* Annotation, *Liability of Public Accountant*, 46 A.L.R. 3d. 979, 92 A.L.R. 3d. 396 (1988).

241. *See* sources cited *supra* note 239.

242. *See id.*

243. *See* sources cited *supra* notes 171 and 201.

Generally, the corporation will be the cheapest cost avoider.[244] Thus, the foreseeable reliance of outside parties on a corporation's computer records may be legitimately incorporated into a negligence standard for computer disaster recovery.[245]

B. *Applying the Standard*

Liability to the corporation — Applying these standards to computer disaster recovery planning, it would seem reasonable that corporate officers and directors have an obligation to consider computer disaster recovery options for their firm. Failure to consider their firm's options and implement their conclusions is failure to safeguard the firm's assets, particularly where information is considered a corporate asset.[246] Such an omission is not protected by the business judgment rule; it falls short of ordinary care to the required fiduciary duty.[247] In most cases, corporate executives have actual notice of foreseeable disasters through their firm's information systems managers.[248] Even where officers and directors have not received actual notice of the importance of computer disaster recovery planning, widespread publicity and government bulletins concerning the subject should serve as constructive notice.[249] Failure to consider a firm's options would therefore result in liability to the corporation or shareholders for losses incurred in a data processing disaster.

Reliance — Parties other than shareholders or the corporate entity may suffer losses due to a corporation's failure to plan for a data processing disaster.. As indicated above, officers and directors are sometimes personally liable in such suits; more often, they will be liable to the corporation for damages it pays in such suits.[250]

The claims of creditors and similar parties against a corpora-

---

244. *See supra* notes 228-230 and accompanying text.

245. For discussion of several possible examples, *see infra* notes 254-265 and accompanying text.

246. *See supra* note 14 and accompanying text.

247. *See supra* notes 184-191, and accompanying text.

248. *See* sources cited *supra* note 20.

249. *See e.g.*, Trimarco v. Klein, 56 N.Y.2d. 98, 436 N.E.2d 502 (1982).

250. *See supra* notes 194-201 and accompanying text. The traditional bulwark against such liability, director liability insurance, has become prohibitively expensive because of the recent expansion of director liability. *See generally* Mallen & Evans, *Surviving the Directors' and Officers' Liability Crisis: Insurance and the Alternatives*, 12 DEL. J. CORP. L. 439 (1987); Special Project, *Protecting Corporate Directors and Officers: Insurance and Other Alternatives*, 40 VAND. L. REV. 775 (1987) (authored by Bennet L. Ross). Disaster recovery measures might contribute to lowering such costs, not only through loss prevention, but by removing some negative factors which require such high costs. *See* Mallen & Evans, *supra*, at 468; *see also supra* note 9.

tion or its executives are somewhat more attenuated than those of shareholders against directors. Generally, these parties may recover from corporations or from corporate executives only where some physical harm has been inflicted upon the victim.[251] As discussed above, courts are reluctant to grant recovery for purely pecuniary losses unless the corporation and its agents were acting as fiduciaries or trustees.[252] This reluctance may stem from a desire to limit liability for increasingly attenuated economic claims.[253] Where physical harm has been inflicted, or where a fiduciary relationship exists, damage to the injured party is considered to be clearly foreseeable. This suggests that third party suits for losses due to lack of a computer disaster recovery plan might be limited to claims against banks or similar financial institutions.

This doctrine may logically be extended beyond financial institutions, however. Information, as indicated above, has become a valuable commodity in our society.[254] No great stretch of the imagination is required to see that firms that store valuable information are in fact acting as trustees or fiduciaries to depositors of information. Medical insurance records, for example, have an obvious value to policyholders who are dependent upon such records to receive medical care. These records are stored by insurance firms as electronic data files.[255] The negligent loss or inaccessibility of such records due to failure of the firm or its executives to prepare for a computer disaster might legitimately be regarded as the loss of a valuable commodity that the policyholder has entrusted to the corporation. Certainly the officers and directors of such a corporation can foresee that harm may result if the records it holds become inaccessible; they should be expected to take reasonable precautions to prevent such harm. Similar arguments may readily be applied to institutions holding educational records, credit records, or other information with obvious economic value.

The value of certain other electronic records is less obvious, but reliance on those who hold them is equally foreseeable. The scientific community has recently given serious thought to committing vast resources to mapping the human genetic sequence.[256] The

251. *See supra* note 201 and accompanying text.

252. *Id.*

253. *See supra* note 232 and accompanying text.

254. *See supra* note 12 and accompanying text.

255. *See* Rhodes, *CICS Early Warning System Helps Keep Blue Cross & Blue Shield Up*, INFOSYSTEMS, March 1987, at 10.

256. *See* Roberts, *Academy Backs Genome Project*, 239 SCIENCE 725 (1988); Roberts, *New Sequencers to Take on the Genome*, 238 SCIENCE 271 (1987).

results of this massive undertaking would be stored as a computer data base.[257] Similar scientific databases already exist, storing information on topics such as AIDS research[258] and drug interaction.[259] Loss of such scientific information due to an unprepared-for computer disaster would be tragic, not only as a scientific setback, but as a waste of the resources already expended. A negligence standard such as that under consideration could serve as an incentive to safeguard such data bases.[260]

Physical Harm — Even absent such a fiduciary obligation, corporations might in many instances be found liable to certain outside parties for negligently failing to safeguard their computer operations. As discussed above, corporations and their agents are held liable for failing to prevent physical harm to outside parties who rely on them.[261] Several of the databases discussed above, such as medical insurance records, are critical to the physical well-being of third parties. Tort compensation generally requires actual harm to occur before a victim may be compensated; the possibility of future harm is not enough.[262] However, cases may arise where persons suffer physical harm because certain critical records are lost or become inaccessible in a computer disaster.

For example, one firm offers bracelets to persons with particular medical conditions; in an emergency where the person is unconscious, health care personnel may call a telephone number on the bracelet to obtain the victim's special medical history.[263] These medical histories are stored as electronic data files.[264] If, because of a computer disaster, these files were lost or even temporarily inaccessible, the victim relying on the bracelet service could die or suffer serious injury. In such a case, the corporation has by contract assumed a duty to the victim.[265] Failure to take disaster recovery measures could leave such a firm, its officers, and directors liable to the victim or her heirs. Adequate computer disaster recovery plan-

257. *See* Roberts, *Who Owns the Human Genome?*, 237 SCIENCE 358, 359 (1987).

258. *See* Batch, *AIDS research Project Buys Critical Time Savings With Communications Pack*, COMPUTERWORLD, Aug. 3, 1987, at S-10, col. 1; *see also* Chester, *CAIN and AIDS*, INFOSYSTEMS, July 1987, 28, 30.

259. *See* Stipp, *Scientists Use Medical Record Data to Detect Adverse Side Effects of Drugs*, Wall St. J., March 24, 1988, at 1, col. 4.

260. *See supra* note 230 and accompanying text.

261. *See supra* notes 171 and 201 and accompanying text.

262. W. PROSSER & W. KEETON, *supra* note 204, § 30, at 165-68.

263. *See* Halcrow, *A Benefit That Saves Money — and Lives*, PERSONNEL J., Feb. 1987, at 10 (describing Medic Alert service).

264. *Id.*

265. *See e.g.*, Texasgulf Inc. v. United Gas Pipe Line Co., 610 F. Supp. 1329, 1350 (D.C. Cir. 1985).

ning for corporations such as these would serve to forestall such suits, protecting both corporations and those who rely on them.

CONCLUSION

As corporations become increasingly dependent on electronic data processing operations, they become increasingly vulnerable to data processing disasters. Natural disasters may cause loss of vital computer functions or destruction of important corporate records; such losses often result in vast economic losses to corporations and third parties. In certain situations, such losses may result in physical harm to third parties. Statutes requiring disaster recovery planning by corporations may create criminal liability for some executives, but have generally not addressed the issue of economic loss. Corporations and corporate executives who fail to take adequate computer disaster recovery measures may also be found civilly liable for negligence. By formulating such a negligence standard, courts can permit tort law to function as a deterrent to these potentially large societal losses.