The Family Jewels: Corporate Policy on the Protection of Information Resources

Daniel J. Knauf

Program on Information Resources Policy

Harvard University

Center for Information Policy Research

Cambridge, Massachusetts

A publication of the Program on Information Resources Policy.

The Family Jewels: Corporate Policy on the Protection of Information Resources

Daniel J. Knauf
June 1991, P-91-5

Daniel Knauf is Assistant Inspector General of the National Security Agency. He prepared this study as a visiting research fellow with the Program.

Printing 5 4 3 2 1

June 1991

PROGRAM ON INFORMATION RESOURCES POLICY

Harvard University **Center for Information Policy Research**

Affiliates

ABRH Consulting, Inc.
Action for Children's Television
American Newspaper Publishers Association
American Telephone & Telegraph Co.
Ameritech Publishing
Apple Computer, Inc.
Arthur D. Little, Inc.
Auerbach Publishers Inc.
Bell Atlantic
Bell Canada
BellSouth Corporation
Boice Dunham Group Inc.
Bull, S.A. (France)
Centel Corporation
CMC Limited (India)
Commission of the European Communities
Communications Workers of America
Computer & Communications Industry Assoc.
COMSAT
Cox Enterprises, Inc.
Dialog Information Services, Inc.
Digital Equipment Corp.
DRI/McGraw Hill
European Parliament (Luxembourg)
France Telecom
Gartner Group, Inc.
GTE Corporation
Hitachi Research Institute (Japan)
Honeywell, Inc.
IBM Corp.
Information Gatekeepers, Inc.
Information Industry Association
International Data Corp.
International Resource Development, Inc.
Invoco AB Gunnar Bergvall (Sweden)
I.T. Direction Ltd. (UK)
Kapor Family Foundation
Knowledge Industry Publications, Inc.
Korea Telecom
Lee Enterprises, Inc.
LiTel Telecommunications, Inc.
John and Mary R. Markle Foundation
Mead Data Central
MITRE Corp.
National Telephone Cooperative Assoc.
The New York Times Co.
NEC Corp. (Japan)
Nippon Telegraph & Telephone Corp. (Japan)
Northern Telecom Ltd. (Canada)
Nova Systems Inc.
NYNEX
Ing. C. Olivetti & Co., S.p.A. (Italy)
OTC Limited (Australia)
Pacific Telesis Group
Public Agenda Foundation
Research Institute of Telecommunications and Economics (Japan)
RESEAU (Italy)
Revista Nacional de Telematica (Brazil)
Salomon Brothers
Scaife Family Charitable Trusts
SEAT S.P.A. (Italy)
Siemens Corp.
Southern New England Telecommunications Corp.
State of California Public Utilities Commission
State of Minnesota Funding
TEKNIBANK S.p.A. (Italy)
TFS, Inc.
Tele/Scope Daily
Third Class Mail Association
Times Mirror Co.
Tribune Company
United States Government:
- Department of Commerce
  - National Telecommunications and Information Administration
- Department of Defense
  - National Defense University
- Department of Health and Human Services
  - National Library of Medicine
- Department of State
  - Office of Communications
- Federal Communications Commission
- General Services Administration
- National Aeronautics and Space Administration
- National Security Agency
- U.S. General Accounting Office
- United States Postal Rate Commission

United Telecommunications, Inc.
US West
Williams Telecommunications
Wolters Kluwer

Acknowledgments

Thanks go to the following persons who reviewed and commented critically on drafts of this report:

Richard Banas
R. Bruce Barr
Robert P. Bigelow
Jay BloomBecker
Kevin C. O'Brien
Richard Broome
Barry Butenhoff
Rod Everhart
Martin Glassman
Robert Carson Godbey
Marr Haack
Eugene Irminger
George Jelen
Hank Jones
Charles C. Joyce
Paula L. Katkin
Beatrice Knauf
Richard Kokoszka
Steve Lipner
David R. Lord
William McLukas
Tom McManus
Noel Matchett
John Monahan
Jane Paradise
Marshall C. Phelps, Jr.
Gretta Powers
L. John Rankine
John Reuss
Elliot R. Siegel
Casimir S. Skrzypczak
Bill Winters
Dan Young
Charles Zraket
Paul Zurkowski

These reviewers and the Program's affiliates are not, however, responsible for or necessarily in agreement with the views expressed herein, nor should they be blamed for any errors of fact or interpretation.

Executive Summary

- Corporations today more than ever before depend upon the availability, integrity, and confidentiality of their business information resources. As these systems have become more complex and critical, they also have become increasingly susceptible to a growing variety of threats. This in turn raises the stakes on some basic questions for top management: Do we need to protect these resources, and if so, how and how much? Against whom or what? At what cost?

- Appropriate answers to these questions depend upon a reasonable estimate of the information resources' value, their susceptibility to various types of damage or loss, and the threats to them.

- Armed with such estimates, management has a better chance of selecting the best mix of policies to implement from the available choices:

  - Establishing official corporate protection policies, codes, and practices

  - Educating the work force

  - Buying insurance policies

  - Relying on the protection provided by law, regulations, and industry standards

  - Contracting for security services such as disaster recovery, risk analysis, and computer system security

  - Taking or implementing direct self-protection measures aimed at increased personnel, physical, or technical security

  - Accepting known and unknown risks as a cost of conducting business; passing costs along to customers

  - Reducing or eliminating the information resource

  - Crossing corporate fingers, relying on hope and luck

- A careful examination of an information resource's value is the first step in the process of coming to a common sense protection policy. Although the financial/dollar business value of the resource is the most important factor in the general concept of "value," there are important legal, organizational (or "turf"), psychological, and ethical dimensions as well. For example, the issue of possible corporate liability for failure to exercise a due standard of care in protecting critical corporate information (or employee personal data) may influence the "value" of an information resource, with respect to the need to protect it. Government regulatory requirements may do the same thing. State, Federal, and International law may also influence the need for protection – either by directly requiring

more, or by indirectly requiring less (owing to the protection provided by criminal and civil law).

- The financial/business value of an information resource is best estimated by a mix of quantitative and qualitative techniques.

  - Such a recipe includes the relatively solid numbers based on the cost of an information resource. The main problem with cost data is that it can be difficult to determine accurately, and it normally does not correlate with the "real" value of the resource to the company.

  - The recipe also includes the somewhat less solid, but more useful "direct" financial value – the value an information resource provides in terms of productivity measures such as cost avoidance, cost reduction, new earnings, etc. A look at the flip side (i.e., the negative financial value if the resource is disrupted or otherwise tampered with) is also useful.

  - Finally, the "indirect" financial value of an information resource must be considered. Although usually impossible to quantify, it may represent the most significant real value to the company. "Indirect" value encompasses the intangible benefits of the resource, such as

    - Better product quality
    - Improved communications
    - Tightened coordination
    - Improved decision making

- Once a practical idea of value is developed (e.g., for prioritizing what needs to be protected), careful thought should be given to the susceptibilities of and threats to corporate information resources, and these should be analyzed separately: different threats/susceptibilities are affected differently by the various protection options.

- Threats are defined as the actors that can cause damage to information resources. They may be categorized into chance events (fires, earthquakes, utility outages), hostile agents (insiders or outsiders who have specific hostile intent towards a corporate information resource), and non-hostile agents (the incompetent and incapacitated, agents hostile to someone else – or to no one in particular, such as authors of computer viruses and worms).

- Susceptibilities represent the openness of an information resource to damage of some kind regardless of the threat. Data alteration or disruption, for example, could be caused by a hacker, an earthquake, a power outage, a disgruntled employee, and so on – the actors are different, but the results are similar.

- The more accurately management understands the value of its information resources, and its unique susceptibilities and threats, the more efficiently and effectively it can select appropriate strategies for protection.

Table of Contents

List of Figures

CHAPTER TWO

APPENDIX A

List of Tables

CHAPTER THREE

CHAPTER ONE

INTRODUCTION

Business organizations today use information resources – especially those associated with telecommunications and computers – for an unprecedented variety and number of important functions. These functions may be strictly internal to the organization, or may focus on the outside world of customers, trading partners, regulators, suppliers, banks, and shareholders. Whether it is in the automation of secretarial tasks, the use of executive information systems, electronic mail, FAX machines, cellular radios, computerized accounting, automated manufacturing, voice mail, electronic transactions, and data interchange – whatever – corporate reliance on the effective collection, selection, manipulation, validation, use, transfer, storage, and retrieval of information has never been so heavy.

With increased corporate use of telecommunications and computers has come an increasing dependence on the reliability and integrity of these systems. With an ever-increasing number of their "family jewels" contained in or dependent upon information resources, corporations have necessarily adapted the increasingly important objective of ensuring the availability, integrity, and confidentiality of business information.

Attention to the value, vulnerability, and sensitivity of corporate information resources has recently become more sharply focused, owing to the publicity surrounding events such as the November 1988 computer software "worm," which hit nearly six thousand terminals connected to Internet (a global research network) and caused damages estimated between $1 million and $186 million.[1] Also, the May 8, 1988, fire at

---

[1] Because dollar losses associated with information resources are notoriously difficult to determine, estimates often vary widely. In this case, an extra variable was whether losses were estimated for computers that were <u>in</u>fected with the rogue program, or <u>a</u>ffected by it in some other way.

the Illinois Bell switching station in the Chicago suburb of Hinsdale disrupted communications for entire towns for weeks, and seriously hurt many businesses that depended upon that particular public network.

These and many similar incidents – accidents and natural disasters, attacks by computer "hackers," employee computer crime and abuse, for example – underline both the stakes involved as well as the vulnerability of the information systems themselves.

Top corporate management, therefore, should examine the following questions:

- Do we need to take steps to protect information resources?
- How effective are the available options for protecting these resources?
- What will protection cost – financially and operationally?

Related, but perhaps even more fundamental questions include the following:

- What are the corporate information resources?
- What is their value to the company?
- How vulnerable are they? To what? To whom?

This report is about the development of cost-effective policies for the protection of corporate information resources. Its intent is to identify the major factors a corporation may want to consider in the development of comprehensive policies and protection strategies tailored to particular business environments or management styles.

A problem in identifying these factors is sorting the wheat from the chaff. Many things – and different kinds of things – have a bearing on the matter. It can be difficult to relate them to each other in a way that allows them to be viewed as a unified whole.

One piece of the puzzle deals with threats from natural disasters and human beings. Another piece deals with the susceptibility of information resources to a wide variety of unfortunate actions or events (such as theft, data alteration, and system disruption). Yet a third piece has to do with figuring out what these resources do, and how valuable they are to the company.

Somewhere in the development of a protection policy, management needs to consider its legal implications, such as legal requirements of the corporation, domestic and foreign privacy legislation, protection provided by the law, and liability issues.

Other factors include the organizational or "turf" consequences of protecting information resources, the ethical implications for the corporation and its employees, and the psychological dimensions of corporate protection policies and procedures.

A final piece of the puzzle concerns choosing from the array of protection options available: establishing written company policies and procedures, taking out insurance policies, contracting for back-up and "disaster recovery" services, taking an aggressive legal posture, and employing direct measures to increase personnel, physical, and technical security (for example, encryption, authentication, and audit trails).

The central question, therefore, is how to put all this together in a way that makes sense for a particular corporation. The purpose of this report is to provide one approach to answer this question. The objective is to provide a basis for making sense out of the factors that may influence the choices a corporation makes in protecting its information resources. Its goal is to facilitate a comprehensive management perspective on the entire issue, rather than on its smaller component parts.[2]

---

[2] Although a great deal has been written about elements such as insurance, encryption, computer security, disaster recovery, corporate tort liability, high-tech ethics, and so on, relatively little has been published that attempts to tie these and other considerations together

In order to achieve this goal, this study offers its readers two practical tools. The first is a framework for organizing the many loose ends that affect corporate policy on the protection of information resources, and a discussion of the major elements within that framework. This essentially amounts to the second tool, a checklist of items that top management may want to consider.

The organization of this report corresponds to that plan. The framework for thinking about protecting information resources is discussed first. This section begins with the basic questions: Should we protect our information resources? If so, how much? When? Where? This study initially puts these questions in terms of 1) Do we need to do this? 2) What will it cost? and 3) How adequate is the resulting protection? The study then focuses on the particular question of need, in other words, why bother? This question of need turns out to present an interesting challenge, encompassing a great variety of considerations dealing with value and vulnerability. These are discussed, however, in a simple step-by-step, item-by-item manner within the overall framework.

The bulk of this study is devoted to what could be described as a checklist of factors that management may want to consider in developing a policy for the protection of information resources. Organized more into a series of focused discussions than an actual checklist, this section explores the ins and outs of the two major concepts underlying the question of need – those of value and vulnerability. Following the survey of policy considerations associated with value and vulnerability is a discussion that addresses the many types of protection which a company may want to consider. They range from relatively inexpensive low-tech approaches, such as simply publishing corporate security procedures and practices, to purchasing insurance coverage, to implementing expensive, high-tech network-wide security systems. This report ends with a few brief summary comments.

---

coherently for management consideration.

By providing a comprehensive framework, together with some common-sense checklists, this report may help corporate managers select and weigh which policy considerations (if any) pertain to their individual circumstances, goals, and objectives.

CHAPTER TWO

FRAMEWORK

Perhaps the most difficult part of developing an effective corporate policy for the protection of information resources is coming up with a practical framework with which to order and simplify the many different, and frequently competing, factors which either intuition or analysis suggests have "something to do" with protection. Briefly introduced in the previous section, these factors encompass disparate elements such as insurance policies, encryption protection, legal liabilities, risk assessments, types of hostile and non-hostile perpetrators, types of system susceptibilities, and approaches for putting a dollar value on information and information systems.

Development of an effective, yet affordable, corporate policy for the protection of information resources requires that we not only consider these disparate factors, but also relate them to each other in a practical way that is applicable to a particular corporate environment.

The following framework meets two needs. The first need is to simplify an issue that has become complicated. Because of the disparity of factors that have a bearing on corporate policies for protection in this area, a method is needed to provide a wide-angle, comprehensive view of the total issue.

The second need is for a practical method to evaluate the choices corporations have for protecting their information resources. Current choices are listed below:

- Establishing official corporate protection policies, codes, and practices
- Educating the work force
- Buying insurance policies
- Relying on the protection provided by law, regulations, and industry standards

- Contracting for security services such as disaster recovery, risk analysis, and computer system security
- Taking or implementing direct self-protection measures aimed at increased personnel, physical, or technical security
- Accepting known and unknown risks as a cost of conducting business, and passing costs along to customers
- Reducing or eliminating the information resource
- Relying on hope and luck, where risks are acceptable

The emphasis that a company places on any of the above approaches will be related directly to the nature of the particular information resource, its perceived value, its susceptibility to damaging actions, and the particular threats the company is worried about. The effectiveness of the protection approaches taken by management will, in the final analysis, depend on how closely the protection policy matches the specific values and vulnerabilities surrounding the information resource.

It may be useful to take an analogy from a different kind of security problem. The basic issue of protection policy is not limited to the area of information resources, but cuts across any endeavor that involves something of value which may in some way be at risk due to its vulnerability. Airplanes are a good example. Loaded with passengers or cargo, an airplane represents several kinds of value to people and organizations who have a stake in it, such as owners of the plane or its cargo, or relatives, friends, and employers of the passengers or crew. Also, an airplane has many kinds of vulnerability. For example, it could be struck by lightning, subject to metal fatigue, or damaged by poor maintenance, construction, design, or navigation. It could be hijacked by an extortionist, a mentally deranged ex-employee, or blown up by a terrorist with hostile intent towards a movement, a nation, an airline, even a particular passenger.

We have included the airline example because the current debate over the protection policy to be taken against a specific threat – a

terrorist bomb or other weapon being smuggled aboard an aircraft – illustrates both the complexity of the problem of protecting aircraft and the utility of a framework in which the categorization of (in this example) threats to aircraft allows for a reasonable response by management. Once we have narrowed the concern to the particular threat of a bomb or weapon being smuggled aboard an aircraft at the point of embarkation (already a small needle in a big haystack, much categorization having been previously done), it becomes clear that several basic policy choices are available.

For example, airline and airport management can focus on the instrument of the threat and susceptibility to it, increasing old-fashioned physical security and inspections, and perhaps bringing new technologies on line, such as bomb-sniffing biological or radiated energy detectors. Or management can focus on the perpetrator of the threat by using passenger psychological profiles, beefing up intelligence operations to provide better advanced warning, or increasing the threat of retaliation.[3] Each method brings with it a variety of "costs" as well as a different level of effectiveness. In reality, some mix of these two basic approaches (focus on preventing the action and deterring the actor) will be used.

The point of this analogy is simply to show that having a logical framework for categorizing the specific aspects of the value or (in this example) vulnerability of something can, and does, provide important information on whether a particular protection measure is adequate and worth its cost. If nothing else, it provides a basis for a more focused debate on what direction corporate policy should take.

As suggested in chapter 1 of this report, the first step in the process of answering the question, Do we need to take steps to protect corporate information resources? is to identify those corporate resources that may need protecting. Although a representative list of

---

[3] In the wake of the December 1988 Pan Am Flight 103 disaster, the former emphasis has been associated with U.S. airport security, the latter with Israeli security.

information resources appears in Appendix A, as well as the current version of the Harvard (Program on Information Resources Policy) Information Resources "Map" – either of which may be used as a checklist in drawing up a corporate inventory of information resources – a better approach is for management to systematically consider the basic elements of its operation and the information resources supporting those operations.

One approach is to identify the information resources supporting each organizational, geographical, or functional element in the company. A recent U.S. General Services Administration publication[4] listed one set of factors for management to consider:

- Facilities (buildings, fences, doors, fire detection/suppression systems, electrical equipment, air conditioning)
- Hardware (computers and peripheral devices)
- Systems Software (operating systems)
- Utility/Support Software (file managers, language translators, programmer aids, security/accounting programs)
- Communications (telephone circuits, cables, modems, encryption devices, computers)
- Personnel
- Application Software
- Data

Another way to "cut" information resources is to think about them in terms of the following elements:

- Function (broadcasting, accounting, manufacturing, sales, inventory control, planning, marketing, publishing, R&D, and so on)
- Format (ink on paper, picture on a CRT, magnetic or optical memory, and so on)

---

[4] U.S. General Services Administration, Office of Technical Assistance, Information Technology Installation Security (Washington, D.C.: GPO, December 1988), 5-6.

- Hardware (computers, modems, FAX machines, telephones, PBXs, and so on) to include CONDUIT (telephone lines, optical fiber, microwave and satellite circuits)
- Software (all kinds)
- Content (customer lists, accounting information, technical information, payroll, inventory)

However an individual company approaches this task, it must first identify the information resources about which it can be asked, Do we go ahead and take action to protect these things? **Figure 1** shows that this question typically will be answered on the basis of the responses to these three questions:

1) Do we <u>need</u> to protect this resource?
2) Is the particular action, or combination of actions, <u>adequate</u> for the task?
3) How much will it <u>cost</u>?

The focus of this report is on that most difficult first question: Do we <u>need</u> to protect this resource? If so, how much? Against whom? Against what? In arriving at an effective corporate policy, management must view adequacy and cost as critical elements of the decision process. Adequacy and cost, however, pertain to the protection options available, and these are themselves identified on the basis of the particular values and vulnerabilities of the particular information resource. To avoid a chicken-and-egg circularity, our framework employs a simple four-step decision process, which is illustrated in **Figure 2**. According to this chronological process, management must

1) Identify the information resources;
2) Determine the need to protect them;
3) Identify the protection options;
4) Decide on implementation.

After identifying the information resources involved, management must ask, Do we need to protect them? The answer depends upon an assessment

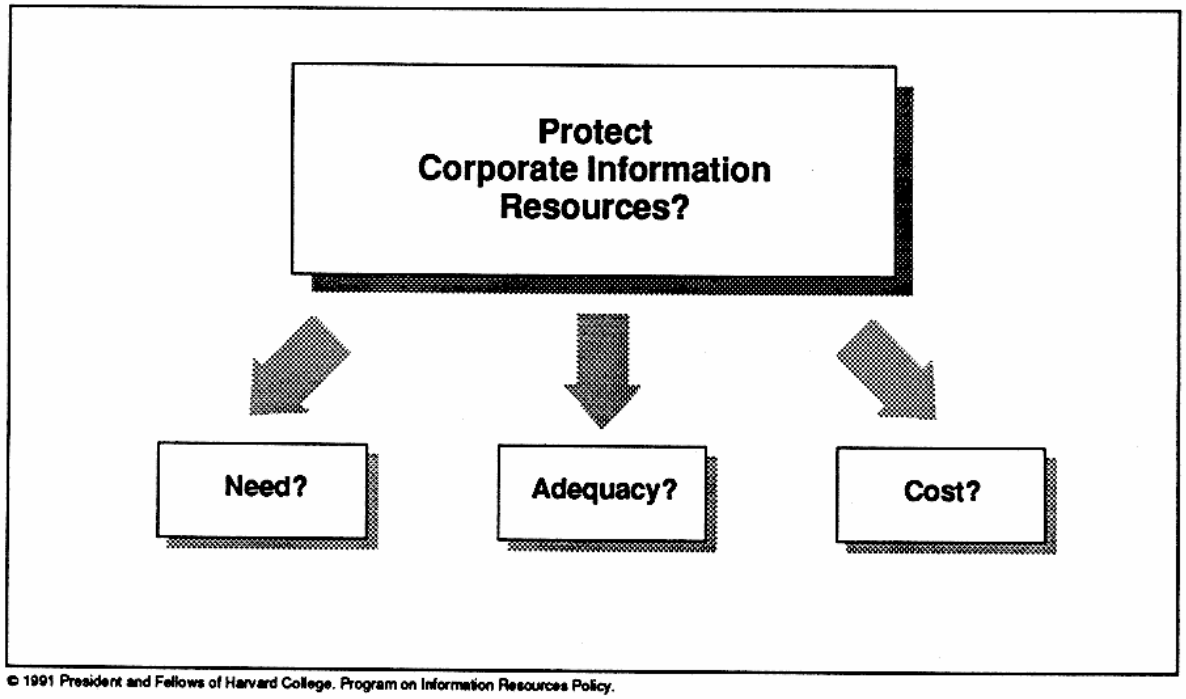

Figure 1

Management Decisions

of two quite different aspects of the information resource – value and vulnerability. The general relationship of these two aspects is shown in **Figure 3**. Very simply, as value or vulnerability increases, so does the need to protect. If either value or vulnerability were ever determined to be zero, there would be no need to protect the asset. Although both aspects will be examined in greater detail in chapters 3 and 4, they are crucial parts of our framework and therefore are diagrammed in **Figures 4, 5,** and **6**.

Figure 4 illustrates several aspects of "value." Some observers have emphasized the dollar/business value and the legal value as most important. Noel Matchett, president of Information Security, Inc., points to the increasing sensitivity of users to the dollar value of the company's information processes (especially in the financial community),

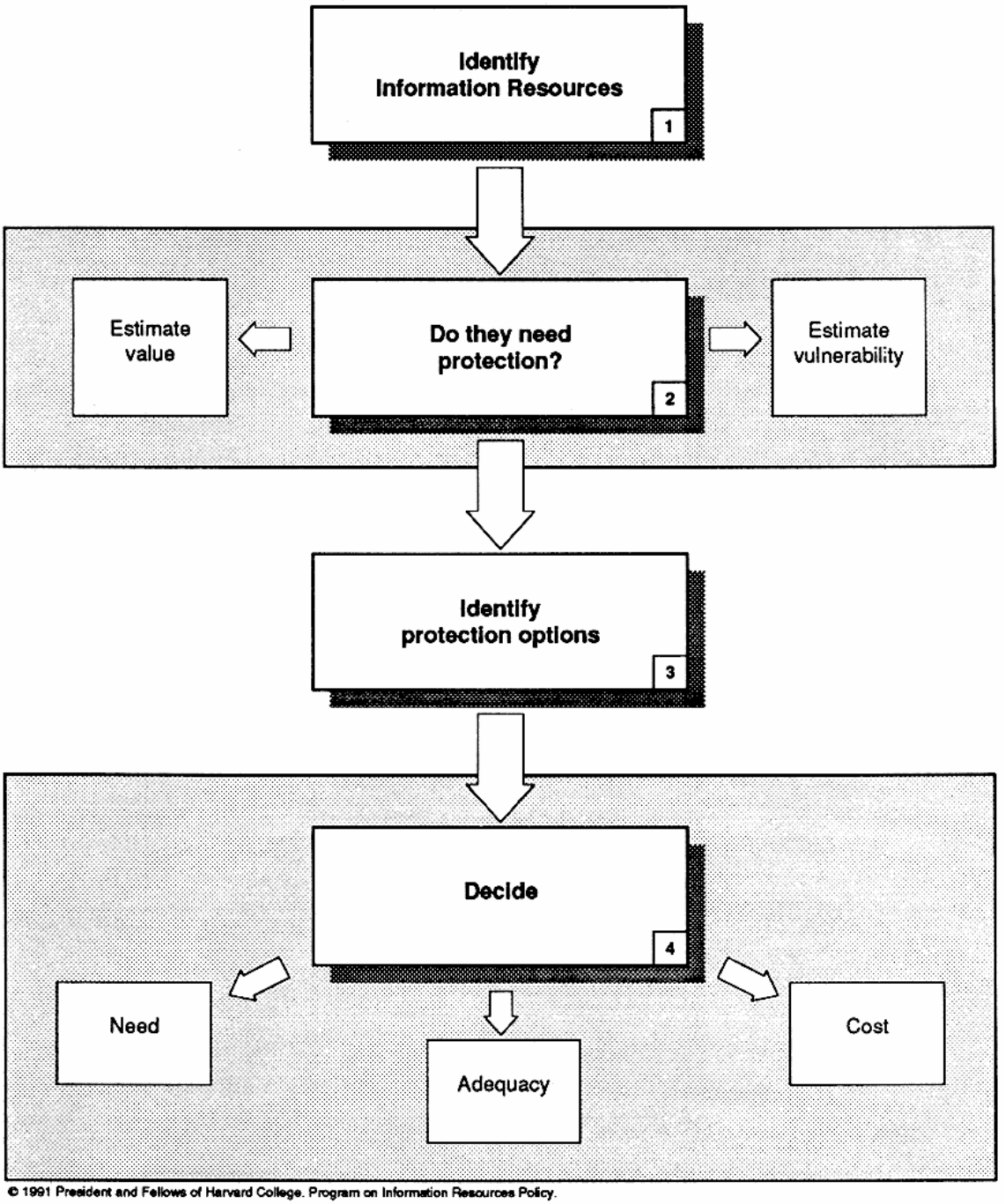

Figure 2

Protection: The Decision Process

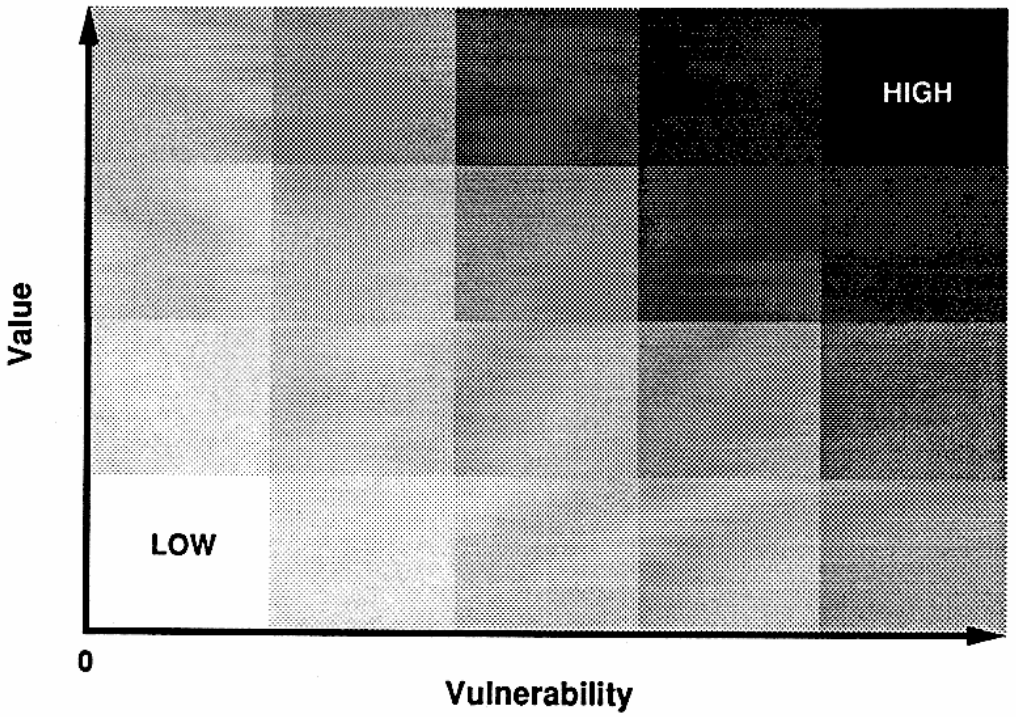

Figure 3

Protection Priority

and the increasing concern over the legal ramifications of protecting information.[5]

Other considerations have also received attention. In estimating the value of an information resource, corporations may want to consider the role that the resource plays within the organization, and the organizational or "turf" impacts that a particular protection action may create. Conducted by the Roper Organization, a recent study of top managers from leading U.S. corporations shows that companies spending more on computers and communications reported seeing these systems influence their organizational structures: almost one-third reported that computers had decreased levels of hierarchy, and 17 percent

---

[5] Noel Matchett, interview with author, February 28, 1989.

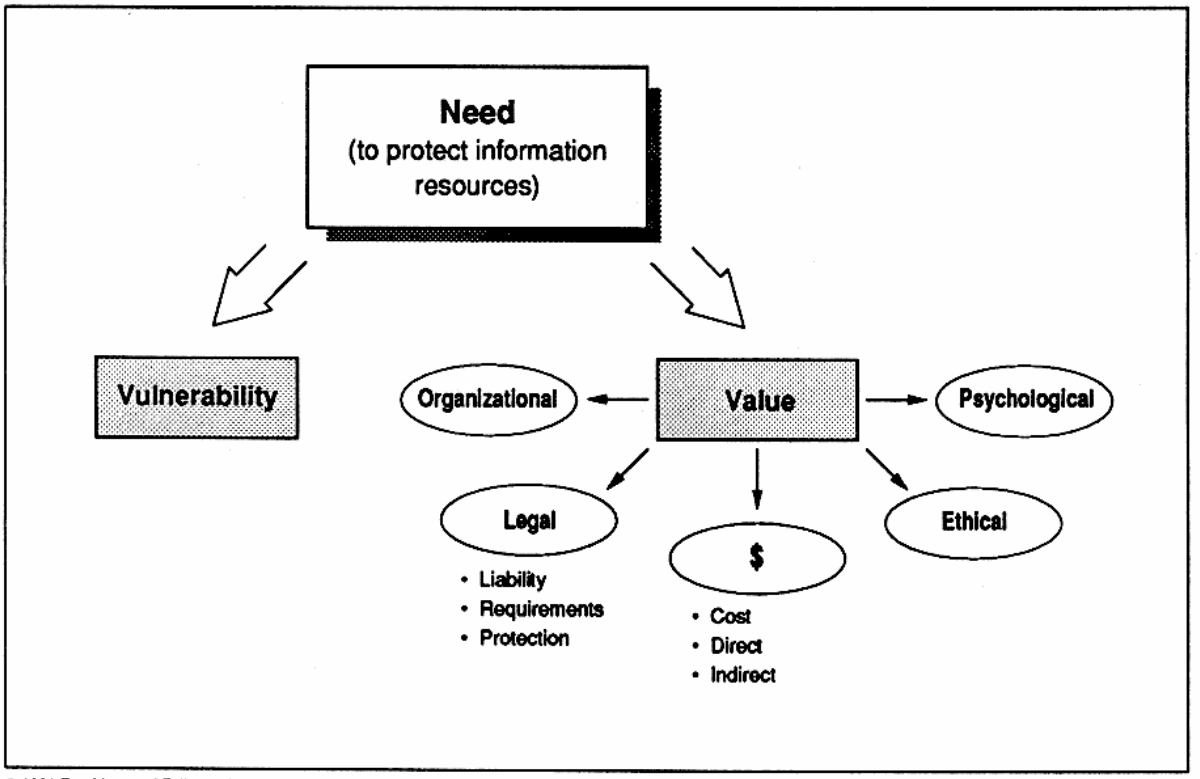

Figure 4

Framework: Value

reported an increased hierarchy.[6] These "turf" dimensions of value may be important when a company decides, for example, to limit the availability of certain types of information to certain groups or individuals.

Further considerations that might play a role in the way a corporation values a particular information resource include psychological and ethical factors associated with the use of that resource. These dimensions can be explored by asking questions such as,

---

[6] "Managing Change: An Executive Perspective on the Enterprise-Wide Impact of Computer Technology," as reported by Wayne Eckerson in "Executives Surveyed About Information Systems," Network World, September 26, 1988, 31.

What psychological "message" would the protection of this asset send to employees, customers, and other stakeholders? One Boston-area corporation recently fired an employee who entered a computer file without authorization by inserting code (a "trap door"), which he could use later to obtain super-user status. A major factor in the company's decision to fire the individual, and let other employees know the reason for the action, was the intention to send such a message specifically to demonstrate the seriousness of the issue.[7]

However, some protective actions may send unintentional psychological messages. For example, ITT once laid off about four hundred employees in its Washington, D.C., headquarters. One step the company took was to disable access codes to an important mainframe-based net for departing employees, fearing possible sabotage. Computer access was denied at 9:00 a.m., but employees weren't told they were being fired until 9:30 a.m., resulting in many complaints about computer downtime. ITT's MIS department head noted that employees now become nervous whenever the system goes down.[8] Another question deals with ethics: Is the nature of this information resource such that there are ethical responsibilities or implications involved? Above and beyond dollar value or legal requirements, significant ethical issues may bear on the protection of certain kinds of information, such as personal medical or financial data.

Most would agree, however, that legal and dollar aspects dominate the more concrete side of the question of value. One set of legal questions deals with the adequacy of law and regulation to protect corporate information. Another set deals with the legal and regulatory requirements on the corporation, to protect certain types of information. And then there is the volatile area of tort law and liability. Credit bureaus have been sued for failing to adequately protect their

---

[7] Charles Zraket, CEO of the MITRE Corporation, interview with author, May 1, 1989.

[8] Crockett, Barton, "People, Not Systems, Key to Network Security," Network World, March 21, 1988, 17.

computers,[9] and banks have been sued for failing to have adequate alternative, or backup, processing capabilities.[10] Attorney Robert P. Bigelow identifies management's stake in liability issues as follows:

> Management, whether it realizes it or not, is responsible for the security of the organization's information system. Sometimes this responsibility is contractual, sometimes it is created by law, and sometimes it will be imposed by the courts. If top management does not act to establish and maintain adequate data security procedures, the organization could be liable for substantial damages . . . and those damages may be collectible from the managers personally![11]

The issue of liability, as well as the current status of federal and state laws, regulations, and court cases is examined in chapter 3. The point here is simply that information resources have a clearly important dimension which can determine their corporate value in a legal sense.

The dollar value (some have defined it the "business value") of information resources is probably the most important consideration in estimating their total "value." This aspect of value is discussed in detail in chapter 3 of this report, but it is important at this point to see where the three types of dollar valuation fit into the overall framework. First, there is the dollar cost of an information resource. In some cases this will be very easy to determine, such as the amount paid for an online data service. In other cases it will be more difficult, such as the costs associated with purchasing, installing, and maintaining an internal electronic mail system. Generally, however, estimating the cost of the resource's value is relatively straightforward.

---

[9] Bequai, August, "Techno-Crimes: Why the Cops Can't Cope," Law Enforcement Technology, March/April 1987, 30.

[10] Campbell, Robert P., "Disaster Recovery: A Significant Business Issue," Datamation, September 15, 1984, Computer Security Institute special supplement, CS1.

[11] Bigelow, Robert P., "Top Management Needs to Know About Data Security and the Law," Datamation, September 15, 1984, Computer Security Institute special supplement.

Cost is only a part of the dollar value, however, and while it may be the easiest to determine, it may have little relationship to the "real" dollar value of the resource to the company. More important are what might be termed "direct" value and "indirect" value. Direct value is used here to describe measurable productivity gains that can be reliably attributed to information resources. Good examples are situations where cost avoidance, cost reduction, or other gains are tied to information technology, as illustrated in a recent New York Times article:

> Since 1978, the New York Stock Exchange has spent $150 million on computers and telecommunications equipment to quicken and expand the process by which stocks are traded. When the modernization program started, the stock exchange employed 1,900 people and could handle 25 million shares on a peak trading day. The stock exchange says it can now handle nearly 430 million shares, with 200 fewer employees.[12]

Direct values are also relatively accurate dollar values, but they tend to have limited applicability. The "real" dollar value of an information resource is frequently of an indirect, intangible nature, which is virtually impossible to quantify. Not that people haven't been trying. As Brandt R. Allen, of the University of Virginia's Business School, recently said, "Thousands of determined executives and thoughtful scholars have grappled with the problem."[13] Unfortunately, much of what has been written on the topic tends to be useless nonsense; typically, apparently "hard" numbers are magically produced out of a subjective fog, and then cleverly manipulated through all sorts of elegant matrices and algorithms.[14]

---

[12] Schneider, Keith, "Services Hurt by Technology: Productivity Is Declining," New York Times, June 27, 1987, D1.

[13] Allen, Brandt R., Measuring Business Value of Information Technologies (Washington, D.C.: ICIT Press, 1988), foreword.

[14] Paul Strassmann, writing on management productivity as an information technology measure, referred to one such valuation taxonomy as "the closest one can get to a modern version of astrology."

Yet, the recognition is widespread that the indirect value of information resources is the most important value. Words such as "strategic resource," "market penetration," and "competitive edge" are frequently called upon to describe this indirect value of information resources. To take but one example, Donald C. Burr built People Express airline but lost it to Texas Air Corporation in April 1987. He attributes his company's downfall to the failure to harness computer technology competitively. His competitors used computer reservation systems that allowed them to set prices at or lower than his own, for specific point-to-point routes. Comments Daniel Cuff, "Once the price value was removed, that took away our competitive edge."[15]

The estimation of dollar value, then, depends on three factors, which range from the relatively accurate "dollar cost," to the less accurate but limited-use "direct" value, to the least accurate but probably most important "indirect" value. And the estimation of value itself must go beyond financial value to at least consider the legal, psychological, organizational, and ethical dimensions of corporate value for information resources.

Figure 5 outlines the other major element – vulnerability – in our framework's approach to the basic question, Do I need to protect these resources? This element is also examined in greater detail in chapter 4, where illustrative examples of specific threats and susceptibilities are discussed. However, a few important points need to be made here. The first is the very sharp distinction, alluded to earlier, between threats and susceptibilities. The concept behind making this division is that looking at the very different types of threat actors can give us a useful means for identifying and evaluating various protective options. So can looking at the range of negative actions to which information resources are susceptible. **Figure** 5 focuses on the threat side of this threat-susceptibility characterization of vulnerability.

---

[15] Cuff, Daniel F., "Builder of People Express Links Failure to Technology," New York Times, October 31, 1988, D4.

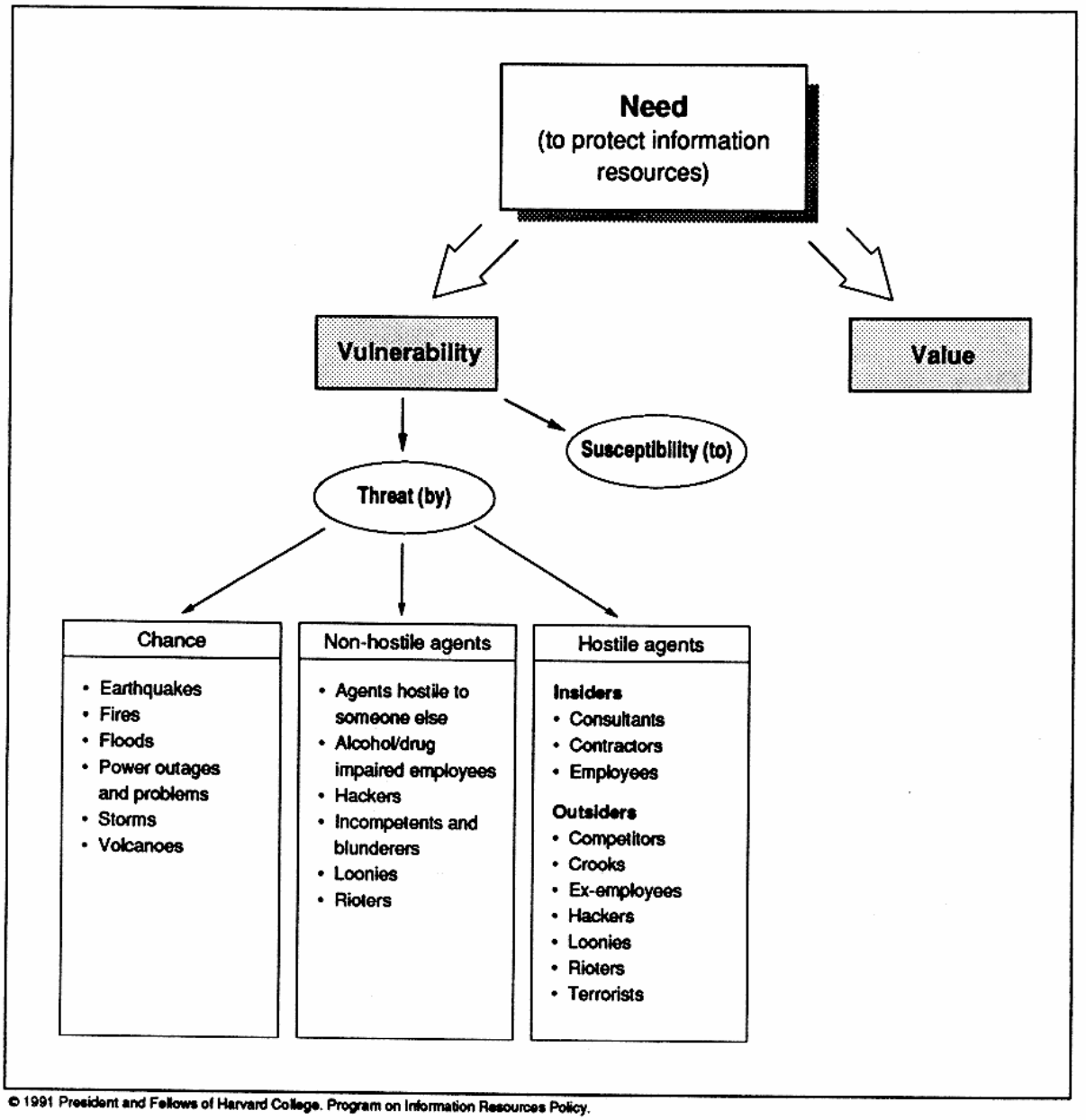

Figure 5

Framework: Vulnerability – Threat

Under "threat" we have three basic categories of actors, or perpetrators. The first group is listed as chance events – "acts of God," such as storms or floods. Deterrence-based protective actions have no effect against these threats; self-defense measures have some

applicability; insurance and backup disaster recovery services have general applicability.

The second group, non-hostile agents, refers to human beings who may not have hostile intent towards Company 1 but may direct hostile intent toward Company 2; in causing trouble for the Company 2, such people may unintentionally cause damage to Company 1. A significant subset of this second group consists of employees or contracted support personnel who may simply be careless, incompetent, poorly trained, or incapacitated, leading to costly – if unintentional – damage.

The third group comprises people who have hostile intent towards a particular company's information resources. These human agents can be outsiders or company insiders. Deterrence-based protective measures may have some effect on these agents, especially company insiders. Self-protection measures may be useful, especially for non-hostile agents and hostile outsiders, but hostile company insiders – especially trusted employees – represent the most difficult group to protect against, even though they may not cause the biggest losses.[16]

Figure 6, on the other hand, focuses on the negative actions that can cause problems for information resources which are susceptible to those actions. These are largely independent of the nature of the threat causing the action. For example, data alteration could be caused by an electrical storm, a careless computer operator, or a hostile and disgruntled employee. Here, too, the type of susceptibility deemed to be significant for a particular corporation's situation will have a direct effect on the type of protective measure selected.

Figure 7 summarizes the "big picture" of information resources of value, which are vulnerable to a wide array of susceptibilities and

---

[16] As noted earlier, the dollar losses caused by crime and abuse involving information resources are notoriously difficult to pin down. Some observers believe that deliberate acts by hostile agents cause the biggest loss; others maintain that losses due to careless accidents are greater.

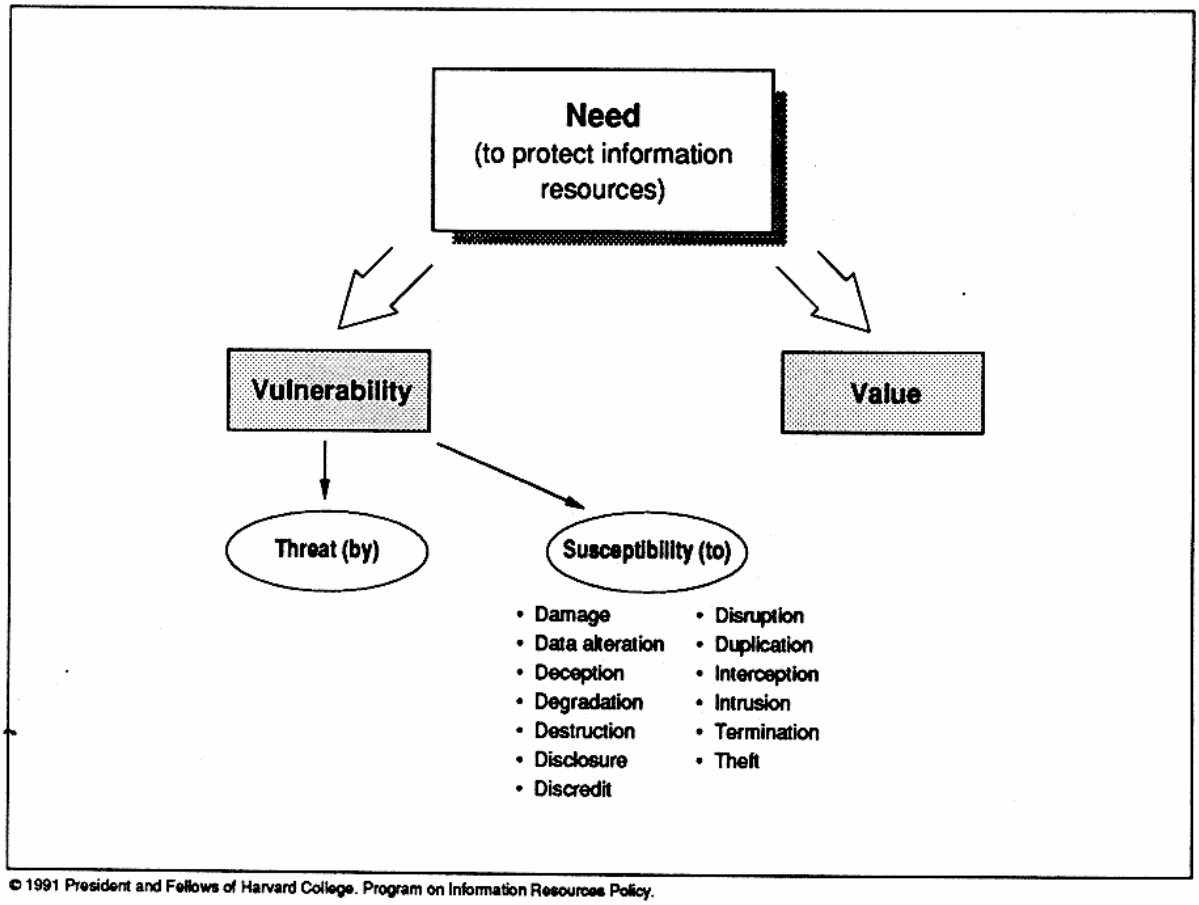

Figure 6

Framework: Vulnerability – Susceptibility

threats. An important added point, however, is that the composite sense of "value" that we have been discussing has meaning only with respect to various stakeholders. We have been using the perspective of the corporate CEO as the stakeholder who, in **Figure 7**, makes the final decisions on the sensitivities of his information resources, in relation to other stakeholders, who might be employees, corporate management, boards of directors, outside regulators, or others. Depending upon one's perspective, different stakeholders could be substituted, for example, individual employee's sensitivities about personal data (contained in information resources) in relation to everyone else.

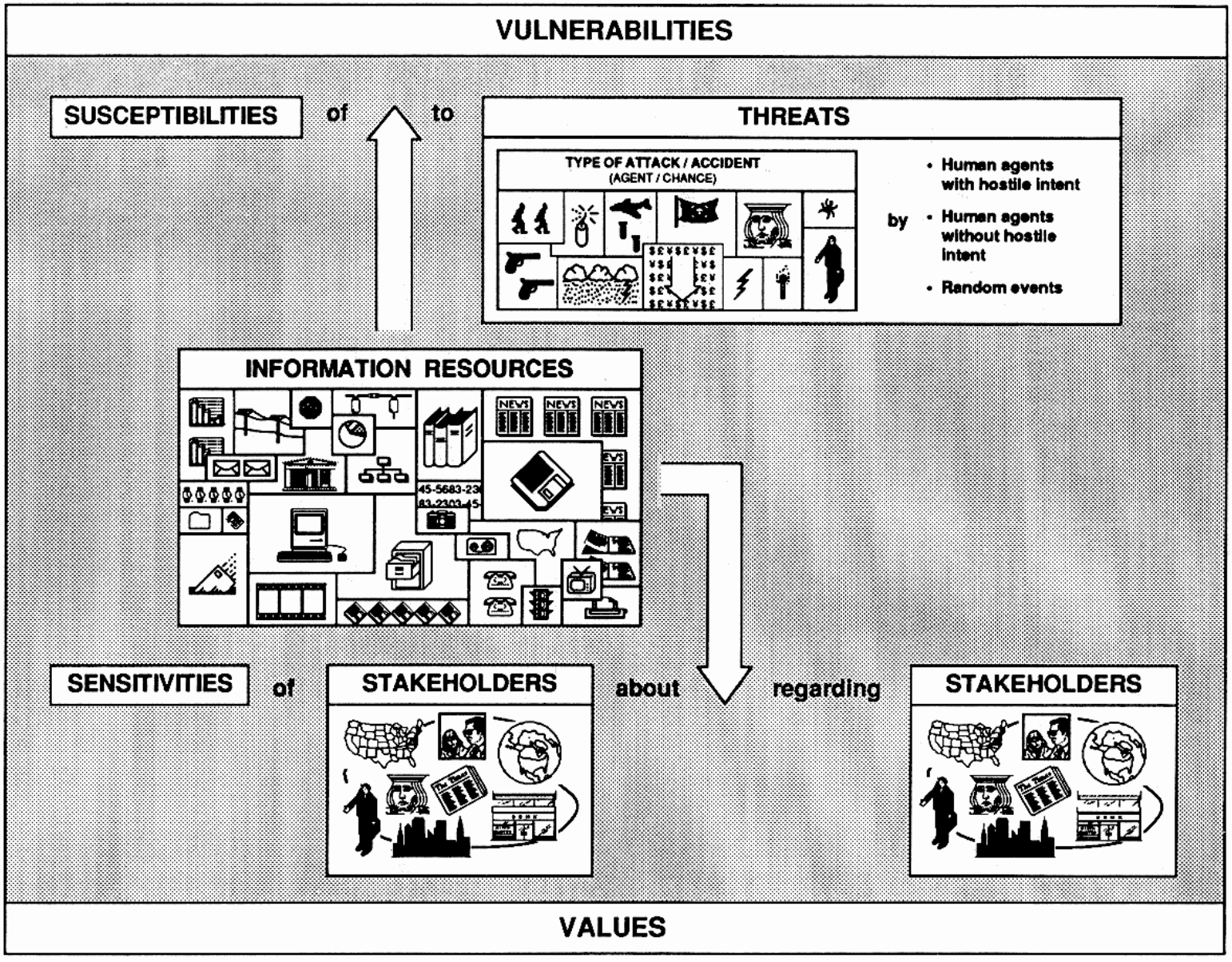

Figure 7

Values, Vulnerabilities, and Stakeholders

Once we have identified and thought through the value and vulnerability of corporate information resources, we can give a rough answer to the question: Do we need to protect these resources? Although the degree of "need" will necessarily be approximate, we can go through a similar process with other identified information resources and gather enough data to develop a reasonable prioritization.

Having accomplished that, the next step is to identify the types of protection methods, and then make a decision based on need, adequacy, and cost. **Figure 8** shows the relationship of these three factors in the final decision. Cost includes consideration of not only the dollar cost to purchase, install, maintain, and operate the protective measure (if these apply), but also the "operational pain" of doing so. Management's judgement of the need and cost, then, must be balanced against the adequacy of the particular protective measure. The generic set of protective measures was outlined earlier in this chapter. The discussion in chapter 5 provides a more detailed checklist of current options. The decision process concludes by weighing any protective measure being considered for its overall suitability and, most especially, for its effectiveness against the particular vulnerabilities (threats and susceptibilities) that are found to be important.

In summary, the proposed framework offers a means to relate the following disparate factors to each other in a conceptual whole:

- Value of information resources, in a broad sense
- Vulnerability of information resources to actors and actions
- Need for protection (again, in a broad sense)
- Costs of protection
- Adequacy of protection

The result is a tool that may prove useful in developing corporate policies for the protection of information resources. Because the individual parts of the complete framework are necessarily approximate –

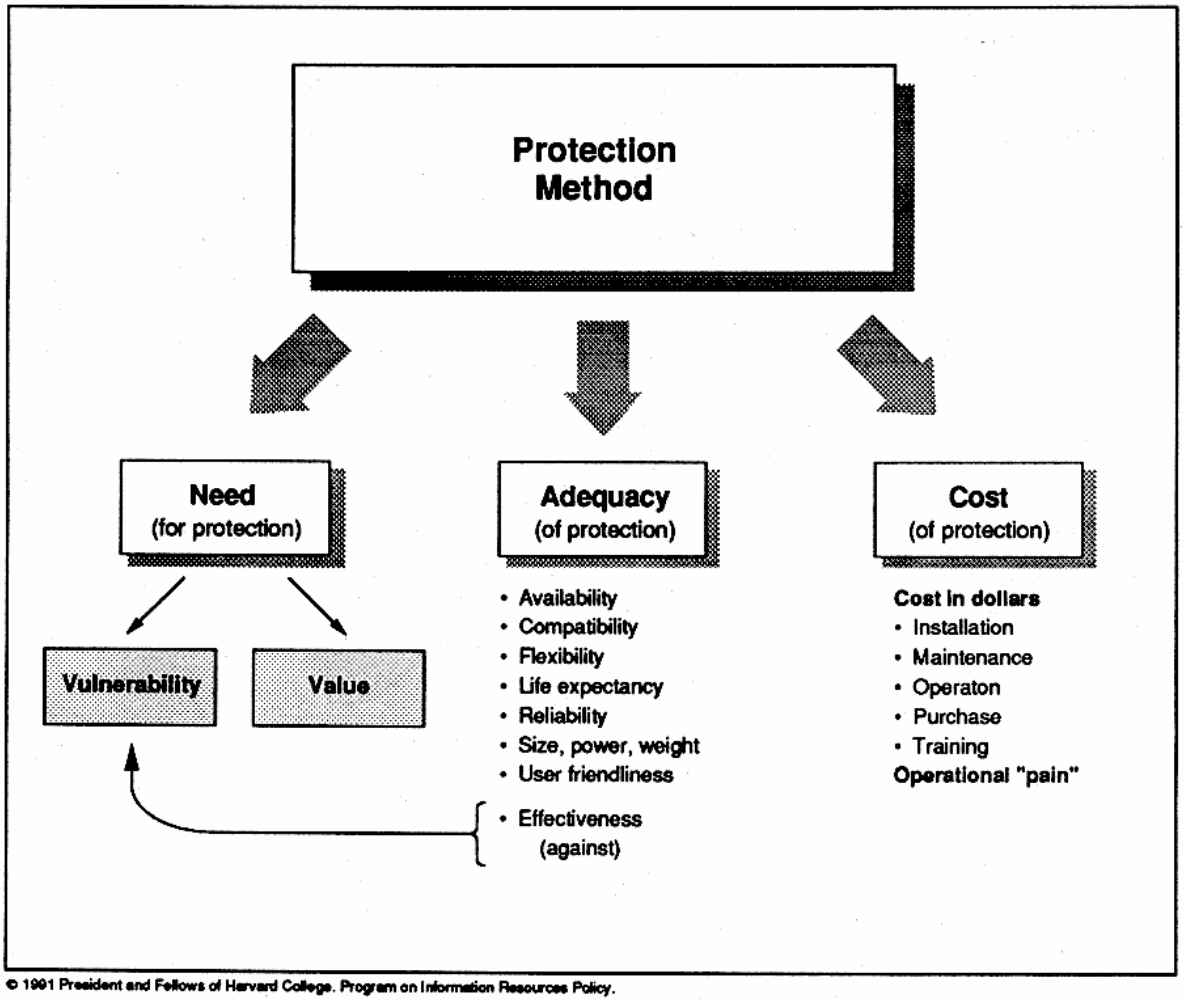

Figure 8

Protection: Need – Adequacy – Cost

none are mathematically precise[17] – the ultimate decision process will be similarly imprecise and approximate.

[17] Given the difficulty "thousands" of scholars have had in producing reliable quantitative measures, one would be well advised to approach any claims of quantitative precision with a keen skepticism.

CHAPTER THREE

POLICY CONSIDERATIONS

This chapter examines the idea of "value" for information resources from several perspectives. It reaches no firm or universally applicable conclusions, but provides – and aims to stimulate – different ways of thinking about value as it may apply to a particular business organization. The most important financial and legal approaches to value are emphasized, but ethical, organizational, and psychological dimensions of value are also considered.

3.1 FINANCIAL VALUE

Because value is a significant factor in identifying an appropriate level of need for protection, one of the best places to start is with the financial, dollar, or business value of information resources. The reason for doing this is simple: a dollar estimate, however rough, can provide a basis for determining how much to spend to protect those resources. Various comparisons to other security-to-value ratios, or insurance rules-of-thumb, for example, could be used as guidelines to establish company policies for protecting information resources. Getting a managerial handle on the financial values of information resources in a useful and practical way, such as one that allows the comparison of the value of one resource to another, requires some means of concise collection and presentation of the relevant data. Without such an organized – and simple – approach, the task quickly becomes a bottomless pit which gets "curiouser and curiouser" the more deeply into it one descends. The question of financial value, therefore, is broken down into the three major elements discussed in chapter 2: cost, "direct" value, and "indirect" value.

3.1.1 Cost

The first aspect of financial value, and generally the easiest to measure in terms of dollars, is cost. Cost figures for a particular information resource may already exist as a budget item, especially if

it involves a neatly-packaged and easily-identifiable contracted service, such as monthly subscription costs for a commercial database, leased communication lines, or leased computer hardware. In most cases, however, the cost will have to be determined after the specific resource has been identified,[18] and will typically involve costs for hardware and software purchase, installation, maintenance, updating/upgrading, and operation. Related to these costs are personnel, overhead, and training costs. Most of these costs can be compared to each other by amortizing them over the expected life of the resource, using standard company procedures.

Some companies approach this task by using simple rule-of-thumb equations. For example, one approach to estimating the total costs of personal computer (PC) systems is to estimate the total number of PC users in the company – some suggest a figure of one-and-a-half to two times the number of installed PCs or workstations.[19] This number is then multiplied by a reference amount (for example, $5000) to calculate overall corporate annual PC cost. According to Ronald Evans et al.

> this estimate – usually far higher than internal estimates – covers many of the hidden costs in personal computing, including the many types of support activities required.[20]

Similar approaches can be applied to different types of information resources.

Another way to look at the cost of a particular resource is to identify its current replacement cost. A cost analysis of an existing

---

[18] The cost does not necessarily need to be identified after the specific resource has been acquired. This discussion, containing references to items such as "current replacement cost," implies a process of costing existing resources. With minor changes, the basic process applies to budgeting for future resources.

[19] Evans, Ronald L., Thomas H. Johnson, and David P. Norton, "What Do PCs Really Cost?" PC Computing, June 1989, 124.

[20] Ibid.

information resource should at least consider the current cost of replacement as one indicator of financial value.

These cost estimates may be listed, totaled, and presented in a simple format such as that shown in **Table 1** – tailored, of course, to the needs and existing practices of a particular corporate environment. In actual practice, simply listing and totaling various costs for an information resource has some drawbacks. In fact, this method may be next to useless for certain types of company assets. For example, the information contained in a corporate database, where the cost to gather, sort, process and store, much less replace, may be very difficult or impossible to determine.

However, even for such information content – as opposed to the more tangible hardware, software, and conduit resources – rough estimates, ranges of dollar costs, and relational cost categorizations (for example, "high" or "low") may be possible using some of the techniques listed in the discussion of "indirect" value (such as expert opinion surveys and focus groups) and should be considered for inclusion on an information resource cost estimate form similar to the one in **Table 1**, above. The important points, however, are that

- Cost is a logical starting place for assessing financial value – giving one perspective on total "value" to the company.
- Cost can usually be determined with fair accuracy for most company hardware and software resources.
- Cost can almost always be determined for contracted or leased products and services.
- A rough cost estimate, a dollar range, or even a subjective categorization as "Very High/High/Medium/Low/Very Low" may be useful in comparing the costs of one information resource to another.

There are two drawbacks to reliance on cost as an indicator of information resource financial value. First, people who conduct cost analysis tend to focus on elements for which it is easiest to find "hard" and defensible cost values; the risk here is that the cost estimate could be biased towards the cost of system hardware and

Table 1

Sample Listing of Cost Estimates

➤ **Information Resource** (company identification) _____

➤ **Description** (function, location, users, responsible organization, etc.) _____

➤ **Amortization Information** (estimated lifetime, amortization period, etc.) _____

➤ **Costs**

Rent/lease	$ _____
Purchase	$ _____
Installation	$ _____
Maintenance	$ _____
Operation	$ _____
Updating/upgrading	$ _____
Overhead	$ _____
Training	$ _____
Other	$ _____
Total costs per time unit	$ _____
Current replacement costs	$ _____

software at the expense of the cost of information. In some cases this bias could seriously distort "real" cost, such as when a cheap floppy diskette containing very expensive data runs on an inexpensive personal computer. This concern is reflected in a Datamation article by Paul Tate:

> In the corporate databases built on those hardware and software platforms lie massive amounts of information representing equally massive corporate investments. That information costs vast sums to gather, sort, process and store, and hopefully it keeps the company competitive. But to accountants it is considered worthless. On the balance sheet,

> information is such a hidden asset it's totally invisible.[21]

A parallel drawback is that emphasizing information resource hardware and software costs may obscure other indicators of financial value, which may be far more significant. In many cases the financial value of information being processed or generated by an information resource is far in excess of the resource's cost, making that cost an unreliable benchmark. An International Chamber of Commerce document, in a section dealing with the value of information resources, emphasizes this point:

> The information, i.e., both data and software, stored in an electronic system is almost always much more valuable than the system itself.[22]

Cost will be used, however, because it provides a general indication of value, and data for the costs of information resources are relatively easy to ascertain. Cost of information resources as a measure of their financial value; rather, this cost should be considered as a potentially useful starting point in estimating value, and by extension, how much to spend on protecting those resources.

3.1.2 "Direct" Financial Value

Certain kinds of information and information systems can yield relatively accurate financial value estimates that are completely independent of the cost of the information or system. Like cost estimates, they provide a means for management to compare the financial value of one information resource to that of another. We have labeled these as "direct" financial value estimates because they lend themselves to more or less direct, quantitative measurement. Several categories or approaches to this use of "direct" financial value:

---

[21] Tate, Paul, "A Badly Needed Sense of the Value of Information," Datamation, March 15, 1989, 78.

[22] International Chamber of Commerce, "Computer Related Crime and Criminal Law: An International Business View," ICC Policy Statements on Telecommunications, Position Paper No. 11, July 1988, Document No. 373/76 Rev.

- Direct dollar values
- Productivity measures (looking at factors such as cost avoidance, cost reduction, new earnings, and so on as a direct result of an information resource)
- Negative financial value through loss, or downtime
- Negative financial value through crime or abuse

3.1.2.1 Direct dollar values

An electronic funds transfer (EFT) is a good example in which the direct dollar value of the information being processed is obvious. The total value of electronic funds transfers in the United States ranges between $1 trillion and $3 trillion every working day. Average individual electronic bank transfers run about $3 million.[23] The clear and obvious financial value of these transactions – together with regulatory requirements – has pushed banking and financial organizations into taking direct steps to protect the hardware, software, conduit, content, and functions associated with each transfer. These steps vary from taking out insurance policies to employing data encryption. A vice-president and data-security officer at Chemical Bank, New York, explains: "We wanted to stay ahead of the problem. . . . We didn't want to start encrypting data after a disaster happened."[24]

3.1.2.2 Productivity measures

Numerous methods in widespread corporate use are designed to measure the increased productivity contributed by a particular factor – be it a person, an organization, incentive award system, or information resource. We will examine their applicability – and frequent lack of applicability – to intangible factors in our discussion of "indirect" value.

However, certain information resources and productivity measurement schemes can, when brought together, yield relatively good estimates of

---

[23] Seaman, John, "Halting Network Intruders," Computer & Communications Decisions, vol. 17 (January 29, 1985), 82.

[24] Ibid.

"direct" financial value. In some cases the resulting financial values can be cranked into traditional business metrics such as Return-on-Investment (ROI), Return-on-Assets (ROA), and Net Present Value (NPV) where dollar returns from an information resource are easily identifiable and measurable. In these cases the financial value of an information resource can be directly compared to that of other corporate assets and investments, which may be useful in balancing corporate expenditures for protection, such as the amount spent on guards or insurance for a fleet of trucks as compared to disaster recovery services for a remote computer facility.

An example might be a financial services business where a simple cost tradeoff is made between the expense of added employees or added processing machines to meet a measurable objective, such as doubling the number of transactions processed in a fixed time. Obviously, the financial value of the processing machine approach, positive or negative, would be the cost difference (cost avoidance) between it and the added-employee approach over some payback period.

In other cases some fancier valuation methods, such as the "Expected Value" theory, "Theoretical Utility," "Incremental Analysis," or "Adaptive Design" prototyping, may be more appropriate where there are more variables and the dollar return is not calculated as easily. An example might be the installation of an automated teller machine (ATM) system, which would have to address the value of different configurations: how many, where located, services offered, and so on.

The common principle underlying all these "direct" approaches to measuring the productivity of an information resource is that of comparing a (past/current/future) business situation <u>with</u> the use of a particular information resource, to as similar as possible a business situation <u>without</u> the use of that resource (or <u>with</u> a different kind of resource, or configuration, or number of them, or different degree of use, or whatever).

Already mentioned are accurately measurable "direct" financial values such as cost avoidance in some manufacturing and service applications of information resources. Certain cost savings can be accurately predicted in advance, or measured during or after-the-fact. An example of advance estimation of direct value is New York Life's recent use of information resources to avoid personnel and overhead costs. The company uses telecommunications and computer technology to process insurance claims in what has been called a "global office." By flying claim forms to Castleisland, Ireland, processing them there on IBM terminals, and then shipping the claim information back to an IBM mainframe in the United States (where letters and checks are automatically mailed to beneficiaries) by way of a trans-Atlantic leased line, New York Life improved its response time while saving substantial, measurable amounts in avoiding the costs of alternative approaches.[25]

Concurrent measurement of the dollar value of cost avoidance can be exemplified by a large firm which put in a human resources information system – essentially a company-wide database. Because the system implementation was spread out over five years, the firm was able to keep year-by-year track of cost data for departments with as well as without the new system. It defined a unit of work as the company's annual cost to process one employee, which included all personnel costs, such as hiring, payroll administration, and transfers. The costs for a unit of work rose 56.1 percent over four years for those departments not using the database, while costs rose only 25.6 percent for departments using the new system. Subtracting system costs from the dollar savings yielded an accurate "direct" financial value in terms of cost avoidance.[26]

There are certainly limitations and pitfalls to using measurements of cost avoidance to determine the financial value of information

---

[25] New York Times, October 18, 1988, D25.

[26] Berger, Paul, "Selecting Enterprise-Level Measures of IT Value," Measuring the Business Value of Information Technologies (Washington, D.C.: International Center for Information Technologies, 1988), 67-69.

resources. For example, it is easy to list as a savings those costs that are improperly valued, would have disappeared on their own, or were avoided for reasons unrelated to the information resource credited with the savings – what Paul Strassmann calls the "fallacy of misplaced attribution."[27] But the biggest problem is that relatively few applications of information resources can be made to fit a cost avoidance model, and the most important business values appear to fall outside the reach of such "direct" measurements.

Still, the direct avoidance of costs in staff, overhead, travel, and so on can generate dollar value for information resources in some important applications. Even in reports of the "downside" of technology we find definable dollar savings in cost avoidance. Over a period of five years, Visa International tripled the number of credit card transactions while increasing its headcount only 30 percent by using up-to-date computer and communications equipment.[28] An article, "The Puny Payoff from Office Computers,"[29] in a contradictory way is replete with non-puny, tangible savings which can be categorized as cost avoidance. New information resources allowed Allied Stores, a major retailer headquartered in New York, to reduce its collections staff by 50 percent while maintaining its number of collection calls made. Productivity doubled. Similarly, Federal Kemper Life Assurance Co. increased its productivity fivefold from 1972 to 1985, as measured by the number of policies issued per employee per year.

An article by Keith Schneider emphasizes the role of information resources in cost avoidance:

> One indication of this is that the phrase "cost avoidance" often comes up when managers and consultants explain what computers have done for productivity. . . . If computers had not been

---

[27] Strassmann, Paul A., "Management Productivity As an IT Measure," 36.

[28] See note 12.

[29] Bowen, William, "The Puny Payoff from Office Computers," Fortune, May 26, 1986, 20.

> improving efficiency somewhere, companies would have needed more white-collar workers to produce the same output.[30]

In addition to the relatively simple use of cost avoidance and similar productivity measures in limited, selected applications, certain kinds of information resource applications develop into separate business or profit-center activities whose financial value can be measured "directly" as profit or loss. A good example is the implementation by American Airlines of its Semi-Automatic Business-Related Environment (SABRE) computerized reservation system (CRS), followed by similar systems established by the other major U.S. air carriers:

> Per dollar spent, the airlines now make more money on their reservation systems than they do flying passengers. According to Edward Stackman, an airlines analyst at Wall Street brokerage Paine Webber Inc., in a good quarter the airlines have an 8 percent to 10 percent profit margin overall, while CRSs make as much as 20 percent profit. In 1984, SABRE netted American a 40 percent profit.[31]

3.1.2.3 Negative financial value through loss or downtime

Another type of "direct" financial valuation is <u>negative</u> in nature, because it is based upon the dollar <u>losses</u> that are lost in the event of the interruption or degradation of an information resource. In this sense these financial losses are a mirror image of the "cost avoidance" savings discussed previously. Like their mirror image, these "direct" losses are relatively easy to quantify, and they suggest the financial value of a particular information resource, but they also have relatively limited applicability. We can get this additional perspective on "direct" financial value by taking a brief look at some actual dollar costs of system loss or downtime.

---

[30] Ibid.

[31] Belitsos, Byron, "MIS Pilots the Air Wars," <u>Computer & Communications Decisions</u> 20, no.3 (March 1988), 36.

The May 1988 fire at the Hinsdale, Illinois, telephone switching center (referenced earlier) stands out. Although the total losses – "direct" and "indirect" – are well into the tens of millions of dollars,[32] certain easily quantifiable losses were the direct result of the accidental fire. For example, one result of the switching center being knocked out was that computer links were interrupted between O'Hare airport's control tower and the FAA center, which directs air traffic control in the area. This interruption in communication necessitated a safety extension of the usual five-mile separation between arriving aircraft to a twenty-mile separation – which in turn caused traffic backups across the nation as well as cancellation of 20 percent of O'Hare's 2,300 flights for that day.[33]

Another example of the direct negative value caused by an information resource downtime is the 1985 computer problem at the Bank of New York. In this case a system glitch stopped the bank from delivering government securities to purchasers. The consequent cash deficit forced the bank to borrow $24 billion to balance the books, and although the problem was corrected the next day, the loan cost the bank between $1.5 million and $2 million.[34]

A University of Minnesota study concluded that a majority of area companies would have to shut down most, if not all, of their business operations if they experienced a serious interruption in computing capabilities:

> In the case of a company with annual sales of more than $200 million, the study found that projected losses for the first week of downtime

---

[32] Elsner, David, "No-Call Toll Mounts in West Suburbs," Chicago Tribune, May 13, 1988; and Wall, Wendy L., "Few Firms Plan Well for Mishaps that Disable Computer Facilities," Wall Street Journal, May 31, 1988.

[33] Richards, Bill, "Fire in Fiber-Optic 'Gateway' Sparks Flight Delays, Problems at Brokerages," Wall Street Journal, May 11, 1988, 6.

[34] Block, Ellen G., and Henry D. Levine, "Protecting the Last Mile: The Quest for a Robust Local Exchange Network," Telematics, October 10, 1988, 9.

> would exceed $90,000. Losses would rise to more than $800,000 by the second week and $2 million by the third. The researchers also discovered that human error, not natural causes, accounted for more than 80% of the system malfunctions.[35]

3.1.2.4 Negative financial value through crime or abuse

A large number of cases involving "direct" losses also have been caused by hostile agents bent on criminal or malicious ends. Although this report will discuss the nature of these threats in chapter 4 (dealing with vulnerability), a brief look at the kinds of direct dollar losses which have been involved will give us yet another perspective on the financial value of information resources.

In a recent criminal case in Texas, Donald Gene Burleson was convicted of inserting a virus-like program into his former employer's computer. The program deleted more than 168,000 records of sales commissions. Reconstruction costs had a direct value of $12,000, the amount he was ordered to pay his former employer in a civil suit.[36]

In another case, Security Pacific National Bank of Los Angeles reported the theft of $350,000 from its automated teller machines (ATM) over the three-day Veterans Day weekend in 1988. It was the largest ATM theft ever reported.[37] Clearly, when money is embezzled or otherwise stolen, "direct" losses are easy to calculate. Other recent cases in which dollar amounts were able to be directly determined are described below:

---

[35] Bequai, August, " 'Information Man' Struggles to Control Information Society," Computerworld, November 3, 1986, CB84; and Corliss, Ellen T., "Prepare for the Worst: Contingency Planning Top Priority in Today's Computer-dependent Businessworld," Massachusetts High Technology, November 7-28, 1988.

[36] Elmer-Dewitt, Philip, "Invasion of the Data Snatchers," Time, September 26, 1988, 63; and "Man Sentenced in Nation's First Virus-Related Criminal Court Case," Compuserve's "Online Today," October 23, 1988, OLT-598.

[37] Cauchon, Dennis, "Holdup Took 3 Days: Take Was $350,000," USA Today, December 1, 1988, 1.

- A clerk at Magnetic Peripherals Inc., a subsidiary of Control Data Corp., stole $150,000 by making up computer invoices from a fictitious vendor company.[38]

- More than $200 million was stolen from Saxon Industries and its shareholders[39], $21.3 million from Wells Fargo, $270 million from Chase Manhattan, and $10.2 million from Security Pacific National Bank.[40]

- Kevin David Mitnick became the first person charged – and convicted – under the federal Computer Fraud and Abuse Acts of 1984 and 1986. He had illegally entered Digital Equipment Corp. computers in Massachusetts, causing between $100,000 and $200,000 in downtime and restoration damages.[41]

In the case of Saxon Industries, the company went from being number 381 on the Fortune 500 list to Chapter 11 bankruptcy in a celebrated fraud case, which depended on "cooking" the firm's computer books.[42] And Saxon wasn't the only company forced to be sold or go into bankruptcy. National Bonded, a Louisiana-based independent money-order company, was hit by a computer "Trojan Horse" (several lines of undocumented, hostile code) that was inserted by a "friend" who had been working for the company as a consultant. "Direct" losses totalled $141,000 and put the company into a negative bank balance situation, eventually forcing its sale.[43]

In virtually every one of these cases of accidents, errors, crime, and abuse of information resources, the "direct" financial losses far

---

[38] McLellan, Vin, "Of Trojan Horses, Data Diddling, and Logic Bombs," Inc., June 1984, 104.

[39] Ibid.; for $200 million figure, see note 45.

[40] Weinstein, Michael, "Systems Beware: Hackers Want In," American Banker, April 2, 1984, 11.

[41] "Drop the Phone: Busting a Computer Whiz," Time, January 9, 1989, 49; and Savage, J.A., "Hacker Pleads Guilty to Computer Violations, Is Denied Bail by Judge," Computerworld, March 20, 1989, 16.

[42] Stern, Richard L., "Carl Icahn's Lucky Day," Forbes, February 10, 1986, 31.

[43] See note 41.

exceeded the cost of the resource itself. The dollar amounts were not difficult to calculate (after-the-fact), nor was it difficult to tie the loss to a failure, problem, or vulnerability in particular information resources; in other words, "misplaced attribution" posed no problem. As stated earlier, however, the ability to confidently quantify the dollar value of such losses is limited to a relatively small set of circumstances, in the same way that "positive" calculation of cost avoidance is limited in its applicability.

The purpose of this brief survey of direct dollar value, productivity measures, and negative financial values through loss, downtime, crime, and abuse as they apply to "direct" financial value was not to give any hard answers to the problem of financial or business value for information resources. The intention was simply to invite different ways of thinking about financial value that may lend themselves to reasonably accurate measurement. The various considerations underlying financial value which were discussed may or may not apply to particular information resources, or to individual corporate organizations. When they do, they can be listed on a simple form similar to that for the cost estimates in **Table 1**, above.

We have tried to show that while information resource costs frequently may be estimated accurately, and may provide some feeling for value, they are often unrelated to the total financial value of the resource to the corporation. Under the category of direct financial value, we have examined briefly several approaches that offer somewhat less accurate dollar values, but which seem to be closer to the "true" or "real" financial value. We will now turn to the "indirect value" of information resources – where most observers see the largest financial value, and the greatest difficulty in measurement.

3.1.2 "Indirect" Financial Value[44]

> The instinct of most managers – and it's often a good one – is to replace manual operations with computers and then plug the resultant cost-savings numbers into one of many familiar formulas. However, when impacts are intangible and qualitative – as is often the case with information technology – these methods of measurement prove inadequate. The most important benefits from information technology are often the most difficult to quantify.[45]

Just what are these elusive, ineffable intangibles that are supposed to be so valuable, yet seem so difficult to pin down in a way that isn't an affront to common sense and intelligence? Nobody seems to know for sure; they're not only difficult to measure, they're also difficult to define. Yet leadership, integrity, courage, esprit de corps, loyalty, and similar qualities are also hard to define and harder to measure, but we all recognize the essential role they play in the success or failure of all human organizations. In the context of the business value of information resources, some of the intangibles frequently encountered are described (if not defined) in these positive terms:

- Improved decision making
- Increased customer satisfaction
- Higher employee productivity
- Better reporting
- Tightened coordination
- Improved communications
- Stronger competitive advantage
- Increased strategic leverage
- Bigger market penetration
- New business opportunity
- Higher employee morale

---

[44] An excellent short summary of common approaches to measure the intangible values of information resource can be found in Edward Rivard and Kate Kaiser's "The Benefit of Quality IS," Datamation, January 15, 1989, 53. A more ambitious treatment of the subject can be found in Measuring Business Value of Information Technologies, published in mid-1988 by the International Center for Information Technologies (ICIT), Washington, D.C. Several articles in the ICIT publication are noteworthy for their historical overviews and references.

[45] Elam, Joyce, and James Kobielus, "From Mysticism to Management," Network World, June 20, 1988, 23.

- Better product quality
- Added flexibility

Of course, some of these qualities lend themselves to at least indirect quantitative measures. Employee morale, for example, might be measured by turnover, use of sick leave, number of submissions in a "complaint mailbox," and similar indicators. Yet, each measure could also indicate something other than the state of employee morale, such as a toxic condition in the workplace.

We can sense that information resources may have a big payoff in the form of intangible benefits, yet the harder we try to nail them down, the more they seem to slip away. As with our previous analogy of airline security to the protection of information resources, it's probably worthwhile to note that information resources are not the only things that have been subjected to attempted measurement of their intangible values. Current corporate efforts to measure the "real" value of employee benefits, such as day-care support, flexible work hours, wellness plans and maternity (or paternity) leave, are running into many of the same difficulties that apply to information resources: "almost endless variables, subjective evaluations, and the kinds of benefits – such as corporate loyalty – that seem impossible to quantify."[46] And the corporate motivation to develop quantitative measures is virtually identical to that behind the drive for measures of information resources: because money is increasingly tight, capital investments and other expenditures need to be justified and "sold" on something more substantial than a "shoeshine and a smile."

Certainly the major fudge factor – some might consider it the fatal flaw – in the valuation of information resources is the problem of <u>subjectivity</u>. In discussing various methods for determining the value of information, Rivard and Kaiser note that

---

[46] Solomon, Jolie, "Companies Try Measuring Cost Savings from New Types of Corporate Benefits," <u>Wall Street Journal</u>, December 29, 1988, B1.

> each depends on analysts' subjectivity. Similarly, the value of qualitative benefits depends on the subjectivity of analysts, users, and management.[47]

This subjectivity can be, and sometimes is, exercised within a company for transparent political, organizational, or "turf" reasons. For example, in discussing the IBM process (called the Executive Planning for Data Processing, or EPDP method), Strassmann identifies several sources of error stemming from "synthesized variables" – one of which begins with an assessment of workload, and an estimated growth in physical volume of information. It is then adjusted by a factor called "complexity growth." According to Strassman

> [T]o estimate the complexity growth, individual executives – usually heads of functions competing for scarce resources – guess at their growing business complexity.[48]

Multiple variables, often inseparable, are another important contributing factor to the unreliability of many quantification schemes for measuring indirect value. The multiple-variable problem looms largest and is perhaps most clearly understood when we look at measurement approaches that focus on the value-added by management, and the role of supporting information resources such as executive information systems (EIS).

Many such methods have been proposed, but they tend to founder on the rocks separating the human variables from those of the machine. How can one determine, for example, the relative contributions to good management of a decisive (or smart, prudent, experienced, informed, or lucky) human manager, and the quality of the EIS which surrounds that manager? Robert Kauffman and Charles Kriebel obliquely refer to this specific weakness when they write that information technology

---

[47] See note 44, Rivard and Kaiser at 53.

[48] Strassmann, ICIT, 34.

> is notorious because of its pervasiveness throughout the organization. Its contribution depends on other primary input resources, notably people.[49]

In proposing their own scheme, "Data Envelopment Analysis (DEA),"[50] Kauffman and Kriebel acknowledge its similar limitations: "The results from DEA are only as good as the data submitted by management for analysis," and "The general problem every manager faces is defining the business-value linkage for IT."[51]

In his discussion, "Business Value as Justificatory Argument,"[52] E. Burton Swanson perhaps comes closest to a practical approach. He proposes that a well-formed "business case" be used in determining the value of information technology proposals, and that the text of such proposals be evaluated as heavily as the quantitative portions. Essentially rejecting any purely (or heavily) quantitative approach as unattainable, he concludes that

> to measure the business value of information technologies in terms of putting a number on it in the conventional sense is problematic, as all but the most naive will agree.[53]

Swanson's chief conclusion is that both quantitative and qualitative considerations are necessary for measuring the business value of information resources.[54]

---

[49] Kauffman, Robert J., and Charles H. Kriebel, "Measuring and Modeling the Business Value of IT," ICIT, 104.

[50] Ibid. Kauffman and Kriebel describe their scheme (pp. 106-07) as "a nonparametric frontier analysis approach to estimating production correspondences."

[51] Ibid., 116.

[52] Swanson, E. Burton, "Business Value as Justificatory Argument," ICIT, 125-38.

[53] Ibid., 135.

[54] Ibid., 136.

However, although costs and "direct" financial values in many cases can be quantitatively measured, the truly intangible values remain captives of subjective judgement, stubbornly resistant to quantification. Some companies have recognized this difficulty and do not make any serious efforts at a quantitative approach, yet they instinctively understand the value of corporate information resources at the gut level. For example, Martin Glassman, director of Management Services for the Times Mirror Corporation, suggests that his company does not employ such measures of value, yet he clearly recognizes that

> we are in the information business. We have a high awareness of how much computers affect our ability to generate revenues. . . without which we're just dead in the water. No computer – no newspaper.[55]

Once we are willing to give up the search for a quantitative philosophers' stone, there are a variety of approaches that may help to develop qualitative categories (such as "high" and "low") useful for approximate comparison and value prioritization. Rivard and Kaiser's summary, for example, describes various approaches designed to deal with subjective evaluation, including

- Focus groups (a small group to focus on identifying system benefits)
- In-depth interviews of key individuals
- Expert opinion surveys
- The Delphi technique (expert opinion on the probability of events and their likely impacts)
- Observation (random or continuous)
- Review of existing systems to identify benefits
- Profiling expected benefits

These methods basically boil down to common sense efforts to do two things. First, come up with a straightforward listing of the important

---

[55] Martin Glassman, telephone interview with author, August 21, 1989.

benefits, or values, offered by a particular information resource (perhaps limited to some maximum number, such as 5, 7, or 10). And second, provide some sort of individual or group evaluation of what these benefits or values mean. In other words, how important are they subjectively judged to be for the business objectives of the company by a selected individual, group, or organization? This evaluation typically will be accomplished on a scale that is comfortable to those who are doing the judging (for example, 1 to 10, or high/medium/low).

In summary, then, to best assess the business value of an information resource in order to determine its relative need for protection (or for any other reason, such as capital budgeting), the kinds of quantitative and qualitative considerations we have been discussing should be combined onto a single form, possibly similar to that in **Table 2**, for consideration by corporate management. Do this for each significant resource, and then proceed with making the hard choices. According to Swanson

> decisive measures do not come easily; they require a unifying scale. And because values are not easily unified by means of a metric, hard choices often remain just that.[56]

This report now turns to the other major aspect of "value" – the legal value of information resources.

3.2 LEGAL CONSIDERATIONS

In this section we examine significant legal aspects of the protection of corporate information resources. Major questions include

- How adequately do state and federal laws protect my information resources?
- What is the current standard for "due care and diligence" applicable to corporate protection of information resources, and what is the likelihood of civil liability suits for failure to meet that standard?

---

[56] See note 52 at 127.

Table 2

Information Resources: Value

➤ **Information Resource** (identification) _____

➤ **Description** (function, location, users, responsible organization, etc.) _____

➤ **Amortization Information** (estimated lifetime, amortization period, etc.) _____

➤ **Costs**

Rent/lease	$ _____	
Purchase	$ _____	
Installation	$ _____	
Maintenance	$ _____	
Operation	$ _____	
Updating/upgrading	$ _____	
Overhead	$ _____	
Training	$ _____	
Other	$ _____	
Total costs per time unit		$ _____
Current replacement costs		$ _____

➤ **Direct Value**

Savings		
• cost avoidance	$ _____	
• cost reduction	$ _____	
• other	$ _____	
Total savings		$ _____
Increased revenues		$ _____
"Downtime" value (per time unit)		$ _____
Crime/abuse potential loss		$ _____

➤ **Indirect Value**

List of benefits:

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____

Group evaluation: _____

(very high, high, medium, low, very low)

- What statutory or regulatory requirements exist that may require corporate actions associated with the protection of information resources?

3.2.1 Adequacy of State and Federal Statutes

Most state and federal statutes that deal directly with protecting information resources date from 1980 or later. Especially since 1985, the recognition began to grow that more and more valuable information was contained in computers, computer systems, and computer networks, and that this information was vulnerable to abuse by a wide array of persons with motives ranging from the comical to the criminal. A debate broke out that has not yet been resolved: Do we need more statutes that specifically address "computer crime and abuse," or will ordinary statutes against crimes such as negligence, trespass, theft, and embezzlement be sufficient?

Although that debate is still going on – and we will see the reasons for the continuing controversy – in the last few years, all but one state[57] have passed laws penalizing offenses variously described as

- Breach of computer security
- Computer fraud, abuse, crime, tampering, trespass, damage, theft
- Criminal use of a computer
- Interruption of computer services
- Offense against computer equipment or supplies
- Offense against intellectual property
- Theft of services
- Unauthorized use or access
- Unlawful use or access

Appendix B lists the citation for each current state law, together with the citations for relevant federal laws such as the Computer Fraud and Abuse Act. The specific offenses addressed by these laws vary

---

[57] As of mid-1989, Vermont was the only state without statutes addressing "computer system offenses," such as unauthorized access, use, and modification of data. Although New Jersey has such a statute, it only allows for civil remedies and specifies no criminal penalties. Massachusetts has additionally expanded its larceny statute to encompass "electronically processed or stored data, either tangible or intangible," and there may be other changes that bring electronic data under the protection of general criminal law.

considerably on a state-by-state basis, with penalties ranging from class C misdemeanors to class A felonies. Table 3 shows the most important "computer system" offenses[58] that have a direct bearing on how well corporate information resources are protected by state legislation. Of the fifty states

- Nearly all have made unauthorized "access" an offense;
- Slightly less than half also proscribe unauthorized "use";
- The vast majority have specific penalties for unauthorized modification or deletion of data;
- Approximately one-third specifically outlaw the unauthorized disruption or interruption of computer system use.

This appears to be fairly broad coverage for information age crimes of abuse against computers, computer systems, and computer networks. However, a number of factors – and some special provisions – in these laws seem to allow for broad interpretation and flexible application; therefore, their actual meaning and force may not be known until a substantial body of actual cases exists, as illustrated in the following examples:

- Some laws address the <u>attempted</u> crime, as well as the actual commission.
- Many laws have limitations dealing with criminal <u>intent</u>, so that access may be illegal only with intent to defraud, deceive, and so on. Typical is Idaho's law: access is illegal when done with the purpose of "devising or executing any scheme or artifice to defraud; obtaining money, property, or services by means of false or fraudulent pretension, representation, or promises; or committing theft.[59]
- Some of the criminal laws only apply if the aggrieved party has taken specific steps to protect the victimized system, as illustrated by New York's law: "A person is guilty of unauthorized use of a computer when he knowingly uses or causes to be used a computer or computer service without authorization

---

[58] These offenses deal with unauthorized access, use, modification of data, or disruption/theft of services. Many of the laws also address offenses such as permanent damage, physical theft, or use of a computer in a crime, which are not included in Table 3.

[59] Idaho Code Chapter 22, section 18-2202 (1987).

Table 3

State Laws Concerning Computer Crime

State	Access	• copy	• disclose	Use	• steal services	Modify	• add/insert	• delete	Disrupt		Reporting requirement	Trial secrecy	
Alabama	✓		✓	✓		✓		✓					
Alaska	✓						✓						
Arkansas	✓				✓	✓		✓	✓			✓	
Arizona	✓					✓		✓					
California	✓	✓		✓	✓	✓	✓	✓	✓		✓		
Colorado	✓			✓		✓		✓					
Connecticut	✓	✓	✓	✓	✓	✓	✓	✓	✓				
Delaware	✓	✓	✓		✓	✓	✓	✓	✓				
Florida	✓	✓	✓			✓		✓	✓				
Georgia	✓					✓		✓			✓		
Hawaii	✓			✓		✓	✓	✓					
Idaho	✓			✓		✓		✓					
Illinois	✓				✓	✓		✓					
Indiana	✓			✓		✓	✓						
Iowa	✓				✓	✓							
Kansas		✓	✓			✓		✓					
Kentucky	✓				✓	✓		✓					
Louisiana	✓	✓	✓	✓		✓	✓	✓	✓				
Maine					✓								
Maryland	✓			✓		✓		✓	✓				
Massachusetts	✓	✓		✓	✓	✓		✓	✓				
Michigan	✓					✓		✓					
Minnesota	✓				✓	✓							
Mississippi	✓					✓	✓	✓	✓				
Missouri	✓		✓			✓		✓					
Montana	✓			✓		✓		✓					
Nebraska	✓				✓	✓		✓	✓				
Nevada	✓	✓	✓	✓		✓	✓	✓	✓				
New Hampshire	✓	✓	✓	✓	✓	✓	✓	✓	✓				
New Jersey *	✓					✓		✓					
New Mexico	✓				✓	✓		✓					
New York	✓	✓		✓	✓	✓		✓					

*New Jersey's law provides a statutory basis for civil action, but no criminal penalties.

continued

Table 3 (continued)

State	Access	• copy	• disclose	Use	• steal services	Modify	• add/insert	• delete	Disrupt		Reporting requirement	Trial secrecy	
North Carolina	✓				✓	✓		✓	✓				
North Dakota	✓	✓	✓	✓		✓		✓	✓				
Ohio	✓			✓									
Oklahoma	✓	✓	✓	✓		✓		✓					
Oregon	✓			✓		✓		✓				✓	
Pennsylvania	✓			✓		✓		✓	✓				
Rhode Island	✓					✓		✓					
South Carolina	✓					✓		✓	✓				
South Dakota	✓			✓	✓	✓		✓					
Tennessee	✓					✓		✓					
Texas	✓			✓					✓				
Utah	✓		✓	✓		✓		✓	✓		✓		
Vermont													
Virginia	✓	✓		✓	✓	✓	✓	✓	✓			✓	
Washington	✓					✓	✓	✓					
West Virginia	✓		✓	✓		✓		✓	✓				
Wisconsin	✓	✓	✓		✓	✓	✓						
Wyoming	✓	✓	✓			✓	✓	✓					

and the computer utilized is equipped or programmed with any device or coding system, a function of which is to prevent the unauthorized use of said computer or computer system."[60] [Emphasis added]

- Several provisions apply only to certain kinds of information or data. For example, Virginia's crime of "computer invasion of privacy" pertains only to the unauthorized examination of employment, salary, credit, or other financial or personal information.[61]

---

[60] N.Y., Penal Law, section 156.05.

[61] Virginia Code section 18.2-152.5 (1988).

- Many of the laws have cut-offs on either their applicability or the degree of seriousness based upon the dollar value of the information lost, or damage caused.

- Several laws provide a statutory basis for civil action to include, like Arkansas, "loss of profits" under "damages."

- Most states specifically penalize using a computer in the commission of a crime. Some make it a crime to receive, retain, or disclose data that was fraudulently obtained.

- Several states prohibit the unauthorized disclosure of passwords, codes, and similar access devices.

- Almost none of the state laws specifically mentions or addresses computer "worms" or "viruses,"[62] although the language and definitions covered under the "access," "use" and "modification" clauses might be applied. In fact, most of the "access" clauses and definitions are, on their face, broad enough to cover any sort of unauthorized penetration. Georgia's is typical: " 'Access' means to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or computer network."[63]

- South Carolina alone provides a penalty for "computer hacking" – up to a $200 fine and 30 days imprisonment for a first offense, and up to $2,000 plus 2 years for subsequent offenses. Its law defines "hacking" essentially as accessing a computer, system, or network <u>without</u> the intent "to defraud or commit any other crime" after access has been gained.

- A few states incorporate specific statutes of limitation, usually ranging from one to five years after the offense.

In addition to these more or less standard legal approaches and clauses of state law, unusual provisions in a few of them could prove to be very important in determining the actual use of the laws by prosecutors and civil litigants.

For example, only three states – California, Georgia, and Utah – specifically require the reporting of violations. However, these states

---

[62] As of mid-1989, several state and federal bills are pending that specifically address "computer viruses," "destructive computer programs," "computer contaminants," and similar threats to computer systems.

[63] Ga. Code Ann. Article 6, section 16-9-92 (1988).

do not make it a criminal offense or provide for penalties if offenses are not reported. It will be very interesting to see if these reporting requirements have any significant effect; while they do not make failure to report a violation a crime in itself, they do provide a statutory basis for the duty to report on the one hand, and offer immunity from liability[64] if a party does report a violation. The Georgia provision is clear on its civil applicability:

> It is the duty of every business; . . . corporation; or other business entity which has reasonable grounds to believe that a violation of this article has been committed to report promptly the suspected violation to law enforcement authorities. When acting in good faith, such business . . . shall be immune from any civil liability for such reporting.[65]

Such statutory duty could be used as an element in tort law "standards of care" litigation, discussed below.

Just as only three states have provisions directly encouraging reporting, only three states – Arkansas, Oregon, and Virginia – have specifically encouraged reporting by considering the need for secrecy during the judicial proceedings. The Arkansas statute addresses the confidentiality of all parties to an action:

> At the request of any party to an action brought pursuant to this section, the court, in its discretion, may conduct all legal proceedings in such a way as to protect the secrecy and security of the computer, computer system, computer network, computer program, computer software, and data involved in order to prevent possible reoccurrence of the same or similar act by another person and to protect any trade secrets of any party.[66]

---

[64] For example, if a person reports an alleged criminal, who claims to be falsely charged and files suit, the reporter would receive immunity from liability.

[65] Ga. Code Ann. section 16-9-95.

[66] Ark. Stat. Ann. section 5-41-106 (1987).

Our review of these state laws leads to questions about whether they are needed, how effective they are, and whether we need more laws, or simply more specific laws. A wide range of informed opinion attempts to answer these questions.

One view suggests that these statutes were not needed, and may even further complicate or cloud prosecutions. Computer lawyer Robert Bigelow, a founder of the Computer Law Association, believes that the general criminal statutes often were adequate, but simply needed to be applied. In particular, he believes that current law has gone far enough and is more than adequate[67]: "Laws get passed without much analysis of whether they're needed."[68]

He has pointed out, for example, the 1972 case of Ward v. Superior Court,[69] in which an employee of a computer service bureau used a client's password to access a competitor's system and obtain a copy of a valuable proprietary program. The court denied a motion to dismiss his indictment for the offense of stealing a trade secret.[70] His basic view is "The less laws, the better," and that general laws are adequate for "computer crime."[71]

Others take a different view. Carl Felsenfeld, a professor at Fordham University School of Law, maintains that "when one looks at electronic funds transfer, one is faced with the shocking knowledge that

---

[67] Robert P. Bigelow, interview with author, May 25, 1989.

[68] Ibid.

[69] 3 CLSR 206 (Cal. Super. 1972), reprinted in Appendix 3 to Computer Contracts (Matthew Bender & Co.).

[70] Bigelow, Robert P., "Computer Security Crime and Privacy," The Computer Lawyer 6, no. 2 (February 1989), 14.

[71] Bigelow interview. He gave as an example the possible applicability of very old common law doctrines such as trespass quare clausam fregit – "whereby he broke the close" – in which a defendant is subject to damages for entering onto the land of another, to unauthorized access into a modern computer network.

there is no 'law' that deals with this tremendous area of banking."[72] Charles Zraket believes that there should be more, and better, deterrent legislation that identifies what should be protected, what a company is liable for, and what the penalties are for people who violate computer networks. In particular, Zraket believes that since companies can't afford very high technical security, strong deterrent laws could save money that would otherwise be spent on protection.[73]

It would appear that there is a need – at a minimum – for specific legislation dealing with those offenses least likely to be covered under general criminal laws, such as unlawful accessing of a computer system without any particular criminal intent. As Ken Thompson stated in a 1983 Turing Award Lecture: "The act of breaking into a computer system has to have the same social stigma as breaking into a neighbor's house. It should not matter that the neighbor's door is unlocked."[74] Others have suggested extending this analogy to be more accurately described as driving a golf cart through a house on a rainy day. Although nothing may have been stolen, privacy would have been violated, and a mess would have been made that the owner would have to clean up.[75]

Yet as Table 3 illustrates, with few exceptions nearly every state has closed this former loophole, so that the statutory authority to prosecute "computer crime" seems to be well in place – even given the various limitations and exclusions noted earlier. According to Jay BloomBecker, director of the National Center for Computer Crime Data, and a former Los Angeles prosecutor, most current laws can be summarized thus:

---

[72] Baum, Michael, "Return Receipt Requested – Part 2," Network World, July 4, 1988, 35.

[73] Charles Zraket, interview with the author, May 1, 1989.

[74] Quoted in Donn Seeley's "A Tour of the Worm," Department of Computer Science, University of Utah, 1989, 15.

[75] Lynn, M. Stuart et al., "The Computer Worm: A Report to the Provost of Cornell University on an Investigation Conducted by The Commission of Preliminary Enquiry," February 6, 1989.

> If you steal using a computer . . . if you do damage to a computer system . . . [and] if you get access to a computer system and it's like trespass . . . then we're going to punish you.[76]

BloomBecker, Bigelow, and others have suggested a different problem. They propose that although inadequate, the laws simply aren't used – prosecutors aren't bringing computer crime cases to court to a significant extent. Although statistics on the number of state cases prosecuted are difficult to find,[77] many experts agree that, generally speaking, the number is very small.

One major reason is that computer crime is rarely reported. How rarely? No one seems to know, although some estimates suggest that only 20 to 50 percent ever get reported.[78] One potential reason is the fear of publicizing a vulnerability which may not be easy or inexpensive to correct (the Arkansas, Oregon, and Virginia trial secrecy laws may reduce this fear). Another possible cause is fear of civil liability, which could probably be reduced with more widespread immunity similar to Georgia's. Some may feel that existing criminal law doesn't address these offenses, or that it would be too difficult to make a case due to the technical issues involved, or lack of experience and knowledge on the part of lawyers, prosecutors, and judges. Yet, others may fear that their losses may not be looked at as serious damage. Eugene Irminger, Chief Financial Officer at Chicago's CENTEL Corporation, stated that CENTEL's policy is to report crimes to the authorities, but that "it's such a complex crime that sometimes lawyers, and juries and society in general say 'I can't really relate to that as being damage.' "[79]

---

[76] Jay BloomBecker, telephone interview with author, May 5, 1989.

[77] The best source is Commitment To Security, published by the National Center For Computer Crime Data, October 1989.

[78] Hafner, Katherine M. et al., "Is Your Computer Secure?" Business Week, August 1, 1988, 64.

[79] Eugene Irminger, interview with author, May 23, 1989.

Even if a crime is reported, it may not be prosecuted for a number of reasons. Some major reasons are listed below:

- Much of it may have been committed by juveniles who are unlikely to be prosecuted.[80]
- Evidence may not be available or admissible in court.[81]
- It may be hard to prove intent, or even to distinguish between accidents and malicious acts.[82]
- Even the Department of Justice acknowledges that "Investigators, prosecutors, and judges do not have the training needed to become familiar with computer terminology and procedures."[83]

But perhaps the biggest reasons are lack of priority and funding. August Bequai has been especially critical of the lack of funding for training in the FBI, local police forces, and Small Business Administration.[84] BloomBecker also sees lack of funds and lack of priority as the primary reasons for few prosecutions. He describes a recent example in New Mexico, where a system operator of a bulletin board was allegedly victimized by a computer virus that infected his system. He had some evidence of who the perpetrator was, so "He went to the police department, he went to the sheriff's department, he went to the attorney general's office, he went to the FBI, and each one had their own reasons for not bringing a criminal prosecution."[85] The

---

[80] Shea, Tom, "The FBI Goes After Hackers," Infoworld, March 26, 1984, 38.

[81] Mendes, Meredith W., "Privacy and Computer-Based Information Systems," Issues in New Information Technology, Benjamin M. Compaine, ed. (Norwood, N.J.: Ablex Publishing Corporation, 1988), 207.

[82] See note 22 at 25.

[83] U.S. Department of Justice, Bureau of Justice Statistics, Report to the Nation on Crime and Justice, 2d edition NCJ-105506, March 1988, 10.

[84] See note 9 at 31.

[85] See note 76.

reasons were basically those of priority. Too many rapes, too many murders, too many drug cases. Too many "big" problems.

It should be noted that where there is a clear commitment to set aside some funding and to prosecute, the laws seem adequate. The Texas conviction of Donald Gene Burleson is an example. BloomBecker noted that New York has had 10 recorded criminal prosecutions, whereas nearby Pennsylvania has had 485.[86] He speculates that the difference isn't in the laws[87] or actual number of crimes, but in the extent to which Pennsylvania's prosecutors are trained, and push prosecutions.

At this point, it simply may be too early in the history of these state laws to assess their effectiveness – either on the books, or in court. In general, however, with respect to the legal protection available for corporate information resources, it might be fair to suggest the following:

1) The criminal laws appear to be – in most states – at least adequate as written.

2) The actual deterrent effectiveness of criminal laws depends primarily on the willingness of prosecutors to act on them, and of victims to report violations.

3) The willingness of victims to report violations and cooperate in prosecutions may be influenced by legal factors, such as legislative action to provide a statutory basis for a civil "duty to report," immunity when reporting, and confidentiality during subsequent judicial processes.

Given the thin evidence, thus far, of the effectiveness of state criminal law, we shall briefly examine federal statutory law in the same area. Many of the same questions about state law arise for federal law, such as adequacy of the language and its coverage, lack of reporting, few prosecutions, and so on. Yet, several differences are worth noting. The primary federal laws addressing computer system abuse are the

---

[86] See note 77.

[87] If anything, New York's law is more comprehensive than Pennsylvania's.

Federal Wire Fraud Law,[88] the Electronic Communications Privacy Act,[89] and the Computer Fraud and Abuse Act.[90]

The Federal Wire Fraud Law is not specifically addressed to computer systems, but it has been applied effectively to cases involving unauthorized access and retrieval of information on computer networks. For example, in 1978 a former computer security officer was convicted of wire fraud when he remotely accessed and downloaded a valuable program from his former employer.[91] The Electronic Communications Privacy Act makes criminal (and provides for civil remedies) the intentional interception, use, and/or disclosure of electronic communications – digital or aural – that are "not readily accessible to the public."[92] It should be noted, however, that conversations using cordless telephones are considered readily accessible – and that cellular radio communications most likely fall into the same category.

The Computer Fraud and Abuse Act (1984, amended 1986) is generally considered to be the primary federal legislative response to computer crime. It contains provisions against unauthorized access; obtaining certain information and records; using, modifying, destroying or disclosing information in, or disrupting, the use of certain computers; and trafficking in passwords. Although the penalties are substantial, and the basic types of abuse are all addressed, there are very significant limitations and exclusions. The access and disruption provisions, for example, only pertain to systems operated by, or for, the federal government, or federally insured or regulated financial institutions. An important – and broader – provision is that it is a federal crime to alter, damage, or destroy information in a "federal

---

[88] 18 U.S.C. section 1343.

[89] 18 U.S.C. section 2511.

[90] 18 U.S.C. section 1030.

[91] U.S. v. Seidlitz, 589 F.2d 152, 7 CLSR 22 (4th Cir. 1978), noted by Robert Bigelow in "Computer Security Crime and Privacy," see note 70.

[92] See note 70.

interest system." This includes not only any federal system, but also any computer "which is one of two or more computers used in committing the offense, not all of which are located in the same state." Even with the need to prove intent to cause damage and the other restrictions noted above, the law recently has been aggressively applied.

On February 14, 1989, eighteen-year-old Herbert Zinn, Jr., won the distinction of being the first person tried, convicted, and sentenced under the Computer Fraud and Abuse Act. He had hacked his way into AT&T and U.S. military computer systems. Along the way, he stole 55 computer programs. The federal judge sentenced him to nine months in prison, a $10,000 fine, and two-and-a-half years of federal probation. U.S. Attorney Anton R. Valukas had this comment about the case: "The Zinn case will serve to demonstrate the direction we are going to go with these cases in the future. Our intention is to prosecute aggressively."[93]

But despite the substantial penalty and the promise of aggressive prosecution, the investigation of this case took a long time, involved extensive cooperation between many government and private organizations and people, and culminated with a raid of the Zinn residence by the FBI, with AT&T and Illinois Bell security representatives, as well as Chicago Police detectives. It remains to be seen whether this level of resources will be committed to similar crimes in the future.

As of mid-1989, there have only been two prosecutions and convictions under the Act.[94] In March 1989, twenty-five-year-old Kevin David

---

[93] Article by Patrick Townson, "Chicago Phreak Gets Prison Term," quotation taken from DOCKMASTER research network (a government-sponsored network dealing with computer security) X-TELECOM-Digest vol. 9, issue 65. For details of the Zinn case, see also: "Computer Whiz Gets Prison Term," AP, February 15, 1988, PM Cycle; Bozman, Jean S., "Bell Tolls for Shadow Hawk," Computerworld, August 15, 1988, 104; and Alexander, Michael, "Prison Term for First U.S. Hacker-Law Convict," Computerworld, February 20, 1989, 1.

[94] Robert T. Morris, Jr., was subsequently indicted and convicted under the act for creating the Internet "worm" of November, 1988.

Mitnick of Los Angeles pleaded guilty to computer fraud (for entering a Digital Equipment Corporation computer system) and to having unauthorized phone access codes.[95] After his arrest, Mitnick was placed under severe restrictions – an unusual aspect of the case. He was held without bail and was allowed to use the telephone to call only his wife, his mother, and his lawyer, and then only under a guard's direct supervision.[96] This treatment is even more severe than that often given to accused murderers and large-scale drug dealers and, at the least, it suggests a no-nonsense policy once a prosecution is joined in earnest.

In summary, it would appear that

1) Existing federal criminal law appears to be adequate for federal government systems, but written to address private corporate systems only in certain limited circumstances, when included as "federal interest" systems.

2) It is too early to tell what sort of applicability the interstate clause of the "federal interest" provision will have.

3) Few cases have been brought to court, but those few have been vigorously prosecuted.

This report now turns to a discussion of civil law, and especially the interconnected questions of standards and corporate liability.

3.2.2 Liability

The second legal question bearing on the protection of corporate information resources deals with liability. Specifically, what legal standards of "due care and diligence" may exist or are being developed, and how can corporations be held liable for failure to meet those standards? We have seen that various limitations, exclusions, and restrictions are inherent in the language of much computer <u>criminal</u> law. Few corresponding limitations are in the area of civil and tort law – so few that the phrase "the sky's the limit" may apply both in terms of the types of suits that might be brought to court, and the nature and size

---

[95] See note 24, "Hacker Pleads Guilty."

[96] See note 24, "Drop the Phone."

of damages that might be awarded. In this section we will consider some of the history, definitions, legal doctrines, trends, and other factors that may be important to consider in developing corporate policies for the protection of information resources.

Predictions of civil court actions in the "information age" have been around since at least 1960, and have remained more or less constant since then. "In view of the rapid rate at which computers are being introduced throughout our society," states Roy Freed, "the legal impact of that development on questions of liability and evidence and in other areas promises to be substantial."[97]

One potentially important aspect of such civil litigation would deal with the corporation's responsibility to take adequate action to protect its information assets. In 1983 Robert P. Campbell argued that

> we can expect to see individual and/or class-action suits. For example, stockholders might sue a corporation that had to devalue its assets and stock because of computer fraud-related losses. Another scenario might find stockholders filing suit because loss of highly sensitive trade secrets seriously hurt the balance sheet.[98]

Robert Bigelow echoes this concern, noting that corporate boards of directors have a fiduciary responsibility to protect the assets of the company. He maintains that failure to establish and maintain an adequate security program would be a breach of that responsibility, and that directors may be held individually and personally to substantial liability for such a failure.[99] Others have pointed to potential liability for failure to protect sensitive personal data on employees or

---

[97] Arthurs, Rich, "Large Firms Elbow into Booming Area of Computer Law," Legal Times, May 14, 1984, 1, quoting Roy N. Freed in a 1960 Practical Lawyer article.

[98] Campbell, Robert P., "Locking Up the Mainframe," Computerworld, October 17, 1983, ID 1.

[99] See note 11.

outside persons (stored in a credit information database, for example), to control information on electronic bulletin boards, or to protect various types of information from unauthorized modification (such as medical records). According to attorney Daniel Brooks, "The growing array of liability-laden situations is so unbelievable that those who discuss them openly risk sounding like Chicken Little constantly screaming that the sky is falling."[100]

The reasons for these concerns are firmly rooted in the historical expansion of tort law.[101] Although civil tort cases can be traced back to the early history of English common law (in other words, law based upon the cumulative precedents set by individual cases, rather than by statutory legislation), they really began to pick up steam, so to speak, in the age of machines:[102]

> The explosion of tort law, and negligence in particular, must be entirely attributed to the age of engines and machines. In pre-industrial society, there are few personal injuries, except for assault and battery. The machines and tools of modern man, however, blindly cripple and maim their servants.[103]

And the preeminent machine and tool of modern man is the computer, which similarly has the capacity to "cripple and maim" – especially when

---

[100] Attorney Daniel Brooks, quoted in Joseph Kelly's, "There Are Precedents to be Set and Fortunes to be Made," Datamation, vol. 31 (June 15, 1985), 116.

[101] With its long history, "tort" and "tort law" surprisingly have no single accepted meaning. One reasonably clear definition of "tort" is: "A civil wrong, wherein one person's conduct causes a compensable injury to the person, property, or recognized interest of another, in violation of a duty imposed by law," in Torts: Injuries to Persons and Property, by Edward J. Kinoka (St. Paul, Minn.: West Publishing Co., 1977).

[102] For a broader treatment, see: Friedman, Lawrence M., A History of American Law (New York: Simon and Schuster, 1973). For a critical discussion of the explosion in liability cases since the 1960s, see: Huber, Peter W., Liability: The Legal Revolution and Its Consequences, (New York: Basic Books, Inc., 1988).

[103] Ibid., Friedman at 262.

it is connected to an activity that is "inherently dangerous." George Trubow, for example, has argued that

> large quantities of sensitive, personal information stored where it is accessible to unauthorized persons, can be considered hazardous to those individuals to whom the information pertains.[104]

Robert Bigelow also believes that such liability cases are more likely to arise where there is something inherently dangerous about the information involved, offering as examples air traffic control, medical care, and intensive care monitoring.[105]

The historical expansion of tort cases has led to the basic concept of "due diligence" or "due care and diligence" as the standard expected and required of all persons – both natural and legal – in the exercise of their normal business. This very general standard of care is defined as "that which is required by the circumstances, the rendering of which prevents liability for negligence."[106] The standard of "due diligence" is one that would be exercised by a "reasonable person" under the circumstances, and the basic concept is that such a person would not allow an "unreasonable risk" to occur. Made by Judge Learned Hand, the classic formulation of an unreasonable risk, "when the foreseeable <u>probability</u> and <u>gravity</u> of the harm outweighs the <u>burden</u> to the actor of alternative conduct which would have prevented the harm,"[107] speaks directly to the point of corporate responsibility to protect information resources.

Homeowners, for example, are required to foresee the possibility of a snowfall and to recognize the gravity of the situation should someone

---

[104] Trubow, George B., "Who's Liable for Failure to Protect Data?" <u>Datamation</u>, "Computer Security Issues and Answers," September 1985.

[105] Bigelow interview.

[106] Gifis, Steven H., <u>Law Dictionary</u>, Barron's Educational Series, Inc., Hauppauge, N.Y., 1984, 133.

[107] <u>Conway v. O'Brien</u> (2d Cir. 1940), and <u>United States v.Carroll Towing Co.</u> (2d Cir. 1947).

slip and fall on snow or ice on their sidewalk. Further, the danger of harm outweighs the burden of clearing the snow with an inexpensive shovel (or hired help).

These same principles likely will be applied as a standard of corporate care in the protection of information resources for the following reasons:

1) The publicity given to the frequency of information resource system failures, errors, crime, abuse, and so on would make it difficult to claim that an incident was unforeseen;

2) The inherent value and/or sensitivity of the information resource would make it difficult to claim that the seriousness of disclosure, misuse, and so on was not foreseeable; and

3) The availability of protective measures[108] has greatly expanded, and their financial and operational costs have generally declined.

The problem with this standard, however, is that it is relative, determined by the facts of each case, considered after-the-fact. It is also a standard as seen from the point of view of a judge and jury. As attorney Randall Miller points out:

> You should analyze conduct for adequacy of performance from the point of view of a jury. A court could easily say that a failure to insure corporate assets essential to corporate survival (such as a data center) would be conduct that falls short of the proper exercise of the minimum standard of care.[109]

Emphasizing this last point, Peter Huber notes that "in each case, what counts is not the employer's best assessment of actual danger, but the imponderables of appearances, perceptions, and jury sympathies."[110]

---

[108] See chapter 5.

[109] Miller, Randall C., "Your Legal Liability in a Data Processing Disaster," Mainframe Journal, November/December 1987, 70.

[110] See note 102, Huber at 177.

The history of tort law has come down to this: today, virtually anyone can bring a suit for compensatory and punitive damages for virtually any kind of "injury" against an expanding field of defendants.[111] It is generally well known, for example, that directors of corporations are personally at risk for failure to exercise appropriate levels of care in managing their business. However

> it is not as well known that senior managers, agents and sometimes employees are also at risk. When there is a catastrophic loss because of a data processing disaster, it is likely that the vice president or manager of MIS can be held personally liable for the loss if there are actions he should have taken to avoid the loss, but did not.[112]

When a company's potential liability is being considered, it may prove important to <u>document</u> what was considered, and why certain actions were taken or <u>not</u> taken. Noting that some companies investigate their situation and do something, others investigate and do nothing, and still others simply do nothing, computer lawyer Bigelow underlines the need to document what has been considered:

> If a company decides to stick its head in the sand and do nothing ... it may, in a sense, be better off than a company which has looked into a question and decided not to do anything. But the reason is that the first company can be accused of stupidity, the second company can be accused of taking a conscious risk. The problem I find with that situation is that once the company has done anything to look into [things], and then decides not to, <u>they should document why they don't</u>, because somebody is going to remember ... or somebody is going to turn up damaging documents in the course of litigation.[113]

---

[111] For a discussion of how far this process has gone in actual court cases, see Huber at note 102.

[112] See note 109.

[113] Bigelow interview.

An important question for any corporation trying to limit its potential liability is that of standards. What sorts of standards of care might a court apply for the protection of information resources? One reason why this question might be important is that computer-based technology is increasingly viewed as mature and, therefore, its "practitioners will be held to an increasing standard of care."[114]

How high a standard? No one will know for certain until the decisions are handed down in future liability cases. However, a few aspects of the standards question may provide an outline of things to come. The "due diligence" doctrine, as we have seen, relies on what actions a prudent person should take to avoid "unreasonable risk." The reasonability determination, in turn, may depend on what actions were available and at what cost, as well as on what published or implied industry (or even government) standards exist. Referring to the integrity and confidentiality of commercial databases, George Trubow notes that

> though there are no industry standards regarding what constitutes adequate data protection, it is common knowledge in the computer and information industry that technology available today can provide far more security than many system operators actually use.[115]

In some highly-regulated industries, such as banking, specific standards do exist for the security of particular types of information resources.[116] In other areas, standards for maturing technologies are rapidly developing, as is the case with Electronic Data Interchange (EDI) systems:

---

[114] Baum, Michael, "Signed, Sealed and ... Delivered?" Network World, June 27, 1988, 53.

[115] See note 104.

[116] For example, U.S. Comptroller of the Currency Banking Circular 177 on "Contingency Planning for Electronic Data Processing Support" was published in 1983 and updated in 1987.

> EDI authentication, integrity and confidentiality are receiving increasing attention, precipitating the development of encryption and authentication procedures such as the proposed American National Standard for Electronic Business Data Interchange Security Structures.[117]

The federal government recently has been very active in developing and publishing security-related standards for information resources. According to Robert Bigelow, although developed for the security of government systems, these standards are also relevant to the private sector, and they may be brought up in civil court cases, as were OSHA safety standards.[118] He suggests that the context in court will be: "Have you considered using these standards, and if not, why not?" According to Bigelow

> when an applicable standard or regulation has been ignored, and the organization suffers a substantial loss, the shareholder may have a claim against the board of directors. Failure to use such a standard may also be evidence of negligence when a third party is injured.[119]

Federal government organizations actively involved in this area include the Department of Commerce's National Institute of Standards and Technology (NIST)[120] and the Department of Defense's National Computer Security Center (NCSC), which is part of the National Security Agency (NSA). Both organizations publish numerous security standards and related guidelines.[121]

---

[117] See note 114.

[118] Bigelow interview.

[119] See note 70 at 12-13.

[120] NIST was formerly the National Bureau of Standards (NBS).

[121] An index of standards available is published by The Information Resources Management Service of the General Services Administration (GSA), Washington, D.C. 20405.

Although a corporation's risk of potential liability may be increased if government or industry standards are ignored, in the world of tort law it remains true that adherence to a standard or regulation is no guarantee of protection. Peter Huber has concluded that knowledge of and adherence to such standards is necessary, but not sufficient:

> The long-standing rule, still applied without apology in the courts, is that even the most complete conformity to applicable regulations is no shield against liability.[122]

This was underlined by a Minnesota Supreme Court case involving warning labels on tobacco products. Although the court ruled that placing warning labels on cigarette packs – required by federal law since 1966 – did protect against claims that warning wasn't provided

> the court said that various other claims beyond a failure to warn – involving strict liability for defective design, misrepresentation, and breach of warranty – are not preempted by the federal warning requirement.[123]

A specific area in which developing standards may play a role in corporate liability cases is that of employee rights to privacy. The privacy tort, as currently applied in court, identifies four types of "invasion of privacy" for which legal remedies are available:

1) Appropriation, or the use of a person's name, picture, or likeness as a symbol of his or her identity without compensation;

2) An intrusion upon a person's physical solitude or seclusion;

3) The public disclosure of private facts; and

4) Placing a person in a false light in the public eye by associating that person with beliefs or activities with which that person has no connection.[124]

---

[122] See note 102 at 47.

[123] Brannigan, Martha, "Tobacco Concerns Can Face Liability Suits, Court Rules," Wall Street Journal, April 17, 1989, B2.

[124] Prosser, William L., The Law of Torts (4th ed., 1971), Section 117.

A great deal of uncertainty exists about how this privacy tort may be applied to modern information resources such as databases. Yet, the "public disclosure of private facts" may play an increasingly important role when a company compiles sensitive information about its clients or employees, such as through drug testing, AIDS/HIV blood testing, and employee monitoring. Arthur Miller, of Harvard Law School, identifies privacy as a fundamental right: "The basic attribute of an effective right of privacy is the individual's ability to control the circulation of information relating to him."[125] Perhaps the most basic formulation of privacy rights was offered in the Supreme Court decision in Katz v. United States:[126]

> Justice Harlan, in his concurrence, stated the two-pronged test to determine whether an individual has a right to privacy. The test requires a person to have exhibited an actual expectation of privacy, and that the expectation be one society is prepared to recognize as reasonable.[127]

In civil litigation of privacy issues, therefore, the issue turns on the individual court's interpretation of what is, in the end, "reasonable." As with other areas of tort law, what was reasonable yesterday may not be reasonable today, as noted in the following example:

> A survey by Ira Michael Shepard and Robert L. Duston, members of a management law firm in Washington, turned up 97 jury verdicts against employers in privacy cases from 1985 to mid-1987. Damage awards averaged $316,000. Before 1980 employee suits for invasion of privacy rarely reached a jury.[128]

---

[125] Miller, Arthur, The Assault on Privacy, Computers, Databanks and Dossiers (Ann Arbor: University of Michigan Press, 1971).

[126] 389 U.S. 347 (1967).

[127] See note 81 at 195.

[128] Hoerr, John, "Privacy," Business Week, March 20, 1988, 61.

Columbia University professor Alan F. Westin points out that Americans increasingly believe that the rights they attach to citizenship in the society – including privacy – ought to have their echo in the workplace.[129] Legislators appear to be taking this belief seriously, and are increasingly turning it into law. A recent example is passage by Congress of the Employee Polygraph Protection Act of 1988. This Act severely limited the use of the polygraph by private employers, primarily on the basis of its alleged unreliability and its invasion of personal privacy.

Although some observers remain skeptical that the number of privacy liability cases against corporations will increase,[130] the recent history of increased privacy litigation, the expanding scope of civil litigation, and the increasingly large amounts of sensitive personal data contained in information systems suggest otherwise.

One question bearing on the likelihood of corporate liability – whether for failure to protect corporate information assets, or the sensitive information of employees, clients, and business partners – deals with the direction of civil liability litigation in its general sense. Put another way, is there indeed a "liability crisis" which is out of control, or is this merely a popular misperception of what has been called "folklaw"? Will such civil litigation increasingly reach into the deep pockets of information age companies, or has the corner been turned on ever-expanding litigation, with large compensatory and punitive damages?

On the one hand, there appear to be ever-expanding definitions of what constitutes legally acceptable causes for action, increasingly broad grounds for awarding damages, and decreasing areas of traditional immunity and/or defense. Although recent courtroom action has dealt

---

[129] Ibid.

[130] Meredith Mendes, for example, believes that the common law privacy tort offers minimal protection for individuals in the context of modern information technology.

primarily with personal injuries caused by instruments other than information resources, it appears to be a small step to apply the legal principles involved to injuries resulting from "unreasonable risk" in information resources.

For example, a Pennsylvania court recently awarded $11.3 million in damages to a victim of a handgun accident. Thirty percent of the damages were assessed against the dealer who sold the gun; the jury determined that a dealer is obligated to provide basic demonstration and instruction before allowing a customer to purchase a gun. Craig Berrington, general counsel for the American Insurance Association, says that the case "raises questions about whether anyone selling any product has any sense of certainty about the liability standards that apply."[131]

In another case, a Madison County, Ill., jury awarded $2.3 million to a victim of medical malpractice. The unusual aspect of the case was that $1.02 million of the damages were for the loss of certain "joy of living" activities, such as gardening:

> The award is part of an emerging and controversial trend in wrongful-death and personal-injury cases known as "hedonic damages." Courts in such cases already accept the concept that victims can be compensated for pain and suffering and the diminished ability to enjoy life. Now juries are being asked to attach a dollar amount to the simple pleasures in life that a victim has lost.[132]

In other cases, proof of actual damage – hedonic or otherwise – has been replaced with proving the <u>fear</u> of damage. A Tennessee case involved wastes from a pesticide plant, which found their way into local drinking water. The plaintiffs demanded, among other things, compensation for their fear of contracting cancer in the future. According to Paul Barrett

---

[131] Quoted by Milo Geyelin, "Gun Dealer Is Held Liable in Accident for Not Teaching Customer Safe Use," <u>Wall Street Journal</u>, June 6, 1989, B8.

[132] Geyelin, Milo, "Hedonic Damages Awarded in Personal-Injury Lawsuit," <u>Wall Street Journal</u>, March 23, 1989, B1.

> [U]ntil about three years ago, most courts either would have thrown out such claims of anxiety or would have allowed only nominal awards. But in August, a federal appeals court in Cincinnati approved the award of a total of $207,000 for "cancerphobia" to five people serving as representatives of the class action.[133]

Until recently, parents enjoyed a basic immunity from being sued by their own children (minors), and from limitations on their parental liability for tortious acts committed by their children. Even such time-honored immunities have been weakened by the expanding reach of tort law. A Texas state court recently allowed minors to sue their parents for injuries caused by negligent operation of a motor vehicle. The court held that the law protects the parents only when they are performing "essentially parental" activities, which do not include negligently driving a car.[134] Such cases suggest that the explosion in liability cases which began in the 1960s has not yet run its course, and that more novel uses of tort law may be expected to right an increasingly wide array of wrongs, both real and imaginary.

On the other hand, some believe that a rollback is at hand in the form of a "nascent movement" for tort reform, driven by outrage on the part of individuals, communities, and businesses at what they believe to be excessive litigation and exorbitant compensatory and punitive damage awards. A key element in this movement – to the extent that it exists – is the reestablishment of contract law as more universally binding. As more and more cases had come to be decided by what a court determined to be appropriate risk and liability, rather than what might have been agreed upon under the terms of a negotiated contract, some saw contract law being absorbed by tort law. Some even went so far as to declare

---

[133] Barrett, Paul M., "Courts Lend Sympathetic Ear to Claims for Compensation Based on Cancer Fears," Wall Street Journal, December 14, 1988, B1.

[134] For more information about this case, see: Green, Wayne E., "Personal Injury Plaintiffs Win Rulings in Texas," Wall Street Journal, December 15, 1988, B8; and Allen, Charlotte Low, "Torts Are Taking Over for Morality," Wall Street Journal, June 9, 1989, A10.

contract law dead on arrival at the courthouse.[135] Those who see a "nascent movement" to revive contract law and curb tort litigation point to recent cases in which awards have been limited (especially for punitive damages), contracts have been upheld, and traditional employer rights have been reasserted.

A young man, for example, signed a waiver absolving the Los Angeles YMCA of responsibility for a scuba diving course he took. He was left alone briefly by his instructor and drowned. When his parents sued the YMCA for negligence, a state appeals court terminated the suit solely on the basis of the signed waiver.[136] Blair G. Childs, executive director of the American Tort Reform Association, believes that "we are finally seeing some areas where the courts are realizing they need to pull back."[137]

In a case that may prove to have important implications for corporate liability for protecting information resources, Judge Gerhard L. Goettel of New York threw out a suit in which A&P was charged with liability for the 1986 death of a woman poisoned by some Tylenol capsules that had been tampered with. Product-liability defense lawyer Victor E. Schwartz said that "it reflects a trend among some judges to swing back to the notion that we aren't going to hold a [corporate] defendant liable simply because we can't get hold of the real wrongdoer."[138] Some see in such cases a "nascent movement" to curtail corporate responsibility more generally for the harmful actions of others:

> Throughout the 1970s and early 1980s, courts generally expanded corporate liability for the wrongful acts of others. For example, in a number of civil suits, landlords and hotel

---

[135] Gilmore, Grant, The Death of Contract, Law Forum Series, College of Law (Columbus: Ohio State University Press, 1974).

[136] Barrett, Paul M., "Liability Waivers Hold Up in More Sports-Injury Suits," Wall Street Journal, November 11, 1988, B1.

[137] Ibid.

[138] Barrett, Paul M., "Tylenol Tampering Ruling Is Seen Affecting Corporate Liability Issue," Wall Street Journal, November 18, 1988, B8.

> operators were held responsible for violent crimes committed on premises found to be inadequately protected.[139]

Even those who believe that there is a serious movement to curtail liability litigation, excessive damages, and the like see a difficult road to travel in order to make any real changes. They are skeptical that what they see as a liability crisis can be reduced by legislation. A number of judges, lawyers, and legal scholars now call for the courts that created the modern liability law to take responsibility for overhauling it.[140] But a problem in getting the courts to reverse the trend is that tort law is seen as "local": cases typically involve individual victims with a claim against a distant corporation seen by the jury as impersonal, insured, and rich. Judge Richard Neely of the West Virginia Supreme Court admitted (tongue-in-cheek, of course):

> As long as I am allowed to redistribute wealth from out-of-state companies to injured in-state plaintiffs, I shall continue to do so. Not only is my sleep enhanced when I give someone else's money away, but so is my job security, because the in-state plaintiffs, their families, and their friends will re-elect me.[141]

Those who have studied the question, Is there a liability crisis? from the statistical point of view have reached inconclusive results. A Rand Corporation review of product-liability cases filed in federal courts from 1973 to 1986 concluded that although there has been a sharp increase in cases, more than half were filed against relatively few companies.[142] Of the 84,694 total cases filed, about half were aimed at 80 companies.[143] Marc Galanter of the University of Wisconsin conducted

---

[139] Ibid.

[140] Barrett, Paul M., "Courts May Have to Lead Product-Liability Reform," Wall Street Journal, October 7, 1988, B1.

[141] Ibid.

[142] Schmitt, Richard B., "Survey Questions Liability Crisis At U.S. Companies," Wall Street Journal, January 18, 1989, B6.

[143] Ibid.

a similar survey, and concluded that contract cases were increasing faster than tort cases. He found, for example, that by 1986, contract cases made up 18.7 percent of the total filed in federal courts; tort cases made up 16.5 percent.[144] Speaking of litigation in any court, practitioners such as Robert Bigelow have differing perceptions – that contract litigation has increased slowly, while tort and analogous litigation, like infringement of property rights, has gone up more rapidly.[145]

These figures must be treated with caution. Both the Rand and the Galanter studies were limited to a survey of actual federal cases. Most estimates are that more than 90 percent end up settled out-of-court.[146] Also, it is generally believed (and Rand acknowledged) that only a small fraction of liability cases are filed in federal courts – the vast majority are handled in state courts. Frank Schubert, president of the Association for California Tort Reform, surveyed 118 manufacturers in 1987 and found that about half had been sued on defective-products claims within the previous two years – most in state court.[147]

Perhaps the real operant of concern for corporate liability involving information resources is not legal doctrines, or theories about the existence or non-existence of a liability crisis, or of movements to counter such a crisis, but something more prosaic: a lot of trial lawyers make a living out of trying, and settling, tort cases. Many specialize in what could be called information-age law. For example, the Computer Law Association, formed by eight lawyers in 1971, has grown to a membership of 1,193.[148] According to Joseph Kelley, "The legal

---

[144] Barrett, Paul M., "Litigation Boom? Professor Turns Up a New Culprit," Wall Street Journal, October 17, 1988, B1.

[145] Bigelow interview.

[146] Ibid.

[147] See note 142.

[148] Bigelow interview. Membership number is current as of May 21, 1989.

community is well aware of the precedents to be set and dollars to be made."[149]

Given the large number of trial lawyers, a "nascent movement" to roll back current types of liability cases might have the unintended effect of accelerating the search for greener pastures of litigation – including liability associated with the protection of information resources. "If you're going to take lawyers' current market away, and you've still got the same number of lawyers," observes Bigelow, ". . . there's an awful lot of bright ones . . . I think they're going to look around for a new area."[150]

Several miscellaneous legal aspects may be useful to consider briefly when formulating corporate policy for the protection of information resources. First, in addition to class-action lawsuits, we may see plaintiffs essentially selling shares in litigation, a process which could lead to more aggressive attacks on corporate liability. An inventor recently brought just such a suit, raising $750,000 in a patent case which, if successful, could yield up to $100 million. "If you thought limited partnerships were only good for buying oil wells or shopping malls," states Richard Schmitt, "think again." He continues, "These days litigants . . . are selling interests in partnerships and other ventures that essentially invest in lawsuits."[151]

Second, we previously noted that several states make legal distinctions in their criminal laws based on whether or not a computer network or system has been provided some form of technical protection. Such protection – or its lack – may also affect a company's position in

---

[149] Kelly continued: "There are precedents to be set and fortunes to be made. That's why lawyers are swarming to . . . computer law." Datamation vol. 31 (June 15, 1985), 116.

[150] Bigelow interview.

[151] Schmitt, Richard B., "Selling Interests in Syndicated Lawsuits Raises Cash – and Questions over Ethics," Wall Street Journal, October 20, 1988, B1.

civil cases, or in enforcing its own contracts. For example, under tort protection of company trade secrets

> the exertion of substantial efforts by the plaintiff to preserve the secrecy with expectable promise of success, together with a substantial value possessed by the information are all matters to be taken into consideration in determining whether a protectible trade secret exists.[152]

And similarly, if a company wants to enforce a non-compete or non-disclosure agreement with a former employee, it's important to take steps so that, if necessary, the company can show it is trying to protect its trade secrets, rather than simply stifle competition:

> You gain legal protection only if the information is really confidential, that is, unavailable from outside sources. Furthermore, you must treat it as confidential. This means identifying it as confidential and restricting employee access to those who have a legitimate need to know.[153]

Having surveyed the many reasons supporting the probability of – and people predicting – a large number of corporate lawsuits involving information resources, the bottom-line question remains: How many have there been? The answer appears to be obscured by the difficulty in compiling data on state-level cases, and on those settled out-of-court. Some observers, such as August Bequai, maintain that "private individuals are bringing a plethora of lawsuits against businesses that have failed to safeguard their computers."[154]

Others, such as Jay BloomBecker and Robert Bigelow, agree that such cases have been few. BloomBecker relates the case of a California

---

[152] Malone, Wex S., Torts: Injuries to Family, Social and Trade Relations (St. Paul, Minn.: West Publishing Co., 1979), 317.

[153] Manley, Marisa, "The Competitors Within," Inc., September 1988, 137.

[154] See note 35, Bequai at CB84.

credit-reporting firm. Apparently due to the firm's poor security, some parties received credit reports that they were not authorized to have. A plaintiff then brought a case under the Fair Credit Reporting Act – which has a maximum fine of $5,000 – hoping for a class action (with many individual $5,000 claims) to finance the case, but few joined in the suit. At that point the credit reporting firm counter-sued, and the case was quietly settled out-of-court.[155] About the paucity of cases BloomBecker admits, "I don't have a good answer." He continues:

> I'm a little surprised that there are virtually no cases yet which have posed issues of . . . basically . . . liability for inadequate security in the computer context. . . . But certainly in other contexts it's quite clear that liability for inadequate security is a viable cause of action whether it's in tort or contracts.[156]

Three possible reasons suggest why cases involving the protection of information resources are so rare. First, they may or may not exist, but in any case they are pursued at the state level, where data is difficult to develop. Second, they may exist, but are settled out-of-court. Or third, they simply don't exist. In addition, a number of possible reasons suggest why cases are not being brought to court:

- Incidents have not been egregious enough.
- New fields of litigation take time to develop.
- Potential plaintiffs have a tendency to cover up incidents.
- Victims may be adequately covered by insurance, and choose to pass along the loss to their insurer.
- Parties don't want to endure the cost and trouble of a five-year legal struggle.
- Some are concerned about the availability and admissibility of evidence.
- The technical difficulty of proving a case is feared to be too great.

---

[155] BloomBecker interview.

[156] Ibid.

- A point of loss – such as from computers, people, trash bins, and the like – is difficult to identify.
- Encouragement of a recurrence is feared.
- The value, or dollar losses, are not easy to calculate and defend.
- Negligence is generally difficult to prove.
- Some worry about higher premiums or cancelled insurance.
- Some don't have enough resources to mount an effective case.
- Others doubt the technical knowledge and competence within the judicial system.
- Legal inertia is yet another concern; other areas of tort law are well-established or are considered to have "deeper pockets."
- Choices other than taking legal actions are available, such as implementing technical protection, buying insurance, and providing for disaster recovery.

Considering the overall issue of corporate liability, Noel Matchett states that there is "definitely a trend to isolate corporate directors from liability, but they're not aware of potential liability for protection of corporate <u>information</u> assets."[157] Perhaps the reason is that this species of liability has been, and appears to remain, just that – <u>potential</u> liability.

In summary, our survey of liability considerations in the development of corporate policies for the protection of information resources suggests the following:

1) The legal structure, history, and doctrines are in place under which corporate directors and employees may be held liable for the failure to protect information resources.

2) There have been many predictions, but few cases.

3) Information technology is viewed as increasingly mature technology. Together with the increasing value of information, increasing publicity about value and vulnerability, and greater

---

[157] Noel Matchett interview.

availability (and decreasing cost) of security measures, all of these factors suggest that an increasingly higher standard of "due care and diligence" will be applied in corporate management of information resources.

4) Companies should consider documenting whatever review and decision process they apply to the protection of information resources.

Whither liability? Peter Huber speculates: "Though we have gone a great distance, there is no reason to believe that the journey is over. In the first place, the momentum of accumulated logic is likely to keep the system moving for the indefinite future, as newly established legal principles are deployed to open up fresh areas of litigation."[158]

3.2.3 Statutory and Regulatory Considerations

A third question needs to be addressed under our general review of legal considerations: What statutory or regulatory requirements exist that may require corporate actions associated with the protection of information resources?

A complete and detailed answer to this question is beyond the scope of this report, as numerous laws and regulations pertain to certain categories of corporate business. For example, many specific requirements deal with companies under contract to the federal government, especially when sensitive or classified defense information is involved. Such companies may have to deal with a wide range of factors (listed below) that otherwise would not apply to private business:

- Laws
- Office of Management and Budget (OMB) Circulars
- Department and Agency regulations
- Defense Investigative Service (DIS) requirements
- General Accounting Office (GAO) Guidelines
- National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS)
- NIST and Department or Agency Guidelines
- Other documents and requirements invoked under contract

---

[158] See note 102, Huber at 9.

Yet, other corporations may have requirements related to protecting information resources, which are specific to a particular type of business. For example, in 1983 a bank was found liable for dishonored checks because it had not diligently tried to provide alternate processing capabilities. The government's response was for the Office of the Comptroller of the Currency (OCC) to issue Banking Circular OCC-177, "Contingency Planning for Electronic Data Processing Support."[159] The purpose of the circular was to establish OCC policy for bank directors, auditors, and bank examiners, requiring an annual review of the adequacy of disaster recovery for protecting bank records:

> The review is to be carried out by the board of directors. . . . The policy also requires directors to review the methods management has employed to reduce or eliminate the risk. The policy clearly implicates officers, managers and other corporate agents in liability for failure to protect corporate assets. It also exposes them to personal liability if losses occur.[160]

In some cases, statutory and regulatory requirements dealing with the disclosure (and protection) of information may conflict with each other, leaving management with the problem of navigating between them. For example, the Bank Secrecy Act of 1970[161] and its implementing regulations are designed to make financial information that might be useful in criminal prosecutions (such as financial transactions in excess of $10,000) available to law enforcement officials. However, the Right to Financial Privacy Act of 1978[162] prohibits financial institutions from giving information to federal authorities without customer consent or certification of compliance with customer

---

[159] This circular was updated in 1987.

[160] Miller, Randall C., "Your Legal Liability in a Data Processing Disaster," Mainframe Journal, November/December 1987, 73.

[161] (PL 91-508), 12 USC 1730d, 1829b, 1951-1959.

[162] 12 USC 3401 et seq.

notification provisions.[163] Some state financial privacy statutes also require banks to protect customer records from improper disclosure. In a Maryland case,[164] for example, the court found that a bank had wrongfully disclosed customer account information to local police because it failed to obtain the consumer's express or implied consent.

Other Bank Secrecy Act implementing regulations adopted by the OCC include a requirement for national banks to report various crimes and suspected crimes. The OCC form for reporting these crimes lists and describes common federal crimes involving financial institutions, and identifies statutes that might be violated, including "18 USC 1030 - Computer fraud: knowingly accessing a computer without authorization, or using it for unauthorized purposes, including obtaining information contained in records of financial institutions."[165] Generally absent outside the financial community, this reporting requirement may be a consideration in a financial institution's choice of approaches for protecting its information resources.

Financial organizations also may have security obligations placed on them by the Fair Credit Reporting Act of 1971[166]. This act provides certain protections for credit, insurance and employment information:

> For example, a computerized credit reporting service lacked appropriate safeguards to check the validity of information about individuals in its database, and erroneous information was given to a potential credit grantor. Credit was denied, and the credit reporting organization was subsequently held liable under the Fair Credit Reporting Act. While in this particular situation the error resulted from inadequate controls for checking information, the same

---

[163] For a detailed discussion of this particular conflict in regulations, see: Jones, Sarah Elizabeth, "Bank Notes," Bureau of National Affairs's Banking Report, vol. 51, no. 10, 435.

[164] Suburban Trust Company v. Waller (408 A2d Md. 758, 1979).

[165] See note 163.

[166] (PL 90-321) 15 USC 1681.

result might well occur where the information was "amended" by an unauthorized person.[167]

Educational institutions have their own set statutes which might affect their policies for the protection of information resources. For example, the Family Education and Privacy Rights Act of 1974[168] denies federal funding to educational institutions that make unauthorized disclosures of individuals' educational records.

Robert Bigelow also notes that state laws often limit private companies' disclosure of records dealing with personal finances, education, health, employment, and insurance.[169]

These few examples of state and federal regulations are briefly mentioned in order to provide a sampling of the regulations that may affect corporate policies for protecting information resources in various categories of business. They range from very clear, direct requirements for certain kinds of protection (such as OCC 177 and disaster recovery for banks), to more oblique "requirements" (such as the Fair Credit Reporting Act and the possible need to protect credit records from unauthorized modification). When corporations review various statutes and regulations that apply to a particular business – whatever their ostensible purposes and titles – it may be worthwhile to consider them on the basis of their actual or potential implications for protecting information resources.

More generally applicable are the series of federal laws dealing with the regulation of securities exchanges – starting with the Securities Act of 1933, and ending (most recently) with the Omnibus Trade and Competitiveness Act of 1988.

---

[167] See note 11.

[168] (PL 93-380) 20 USC 1232g, 1974. Discussed in Meredith Mendes' "Privacy and Computer-Based Information Systems," see note 81 at 210.

[169] See note 70.

These acts rely on regulated public disclosure as the principal means to achieve their primary purpose of protecting the investing public. The Securities Exchange Act of 1934[170] created the Securities Exchange Commission (SEC) to administer both acts, and required that issuers must register[171] with the SEC prior to offering securities for trade. The registration process entails filing a statement with the SEC containing detailed information on the security, the issuer, and the underwriters. These basic laws were subsequently amended by a series of laws, the most significant of which (for the protection of information resources) was the Foreign Corrupt Practices Act of 1977 (FPCA).[172]

3.2.4 The Foreign Corrupt Practices Act

The FCPA was a regulatory product of the post-Watergate environment of 1977, following in the wake of repeated disclosures of large payments by U.S. corporations to foreign officials, organizations, and individuals. As originally passed, the FCPA consisted of two major parts:

1) "Anti-bribery" provisions,[173] which greatly limited the types of payments that could be made to various kinds and levels of foreign officials; and

2) "Accounting" provisions,[174] which were intended to ensure disclosure to prevent concealment of foreign bribes.

Specifically, under subsection (A) of the accounting provisions, reporting companies are required to "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." Under subsection (B) they are also required to "devise and maintain a system

---

[170] 15 USCS 78.

[171] 15 USCS section 781 (g)(1)(B) requires registration where the issuer has gross assets in excess of $1,000,000 and a minimum of 500 stockholders.

[172] (PL 95-213) 91 Stat. 1494.

[173] 15 USC 78dd-1, 78dd-2 (1982).

[174] Section 102 of the Act, incorporated into the Securities Exchange Act as Section 13(b)(2).

of internal accounting control sufficient to provide reasonable assurances" that the execution and recording of transactions is properly controlled by management.

Shortly after the FCPA went into effect, observers began to see that, despite the act's title, its major impacts might be on practices that were neither foreign nor corrupt. Hurd Baruch states that "the responsibilities – and corresponding liabilities – of corporate officers, directors, and managers under the federal securities laws were greatly increased by the passage of the Foreign Corrupt Practices Act of 1977.[175]

In addition to the CEO and COO, other executives vulnerable for accounting failures were identified as the financial VP, controller, treasurer, tax director, and internal auditor:[176]

> Aimed primarily at illegal corporate acts, like bribes overseas, this law also makes management responsible for its accounting and internal controls. Conceivably, corporations could face legal troubles if they are grossly negligent in applying proper data-processing, auditing and accounting controls and as a result suffer material loss.[177]

In 1987 Randall Miller echoed this view. He claims that under the FCPA, "there is no requirement that the government prove 'scienter'[178] in order to establish a violation. In order to avoid liability, those persons responsible must exercise an <u>affirmative duty</u> with respect to

---

[175] Baruch, Hurd, "The Foreign Corrupt Practices Act," <u>Harvard Business Review</u>, January/February, 1979, 32.

[176] Ibid., 50.

[177] Henkel, Tom, "Policies Cover 'Errors and Omissions': User Suits Give Rise to 'Malpractice' Insurance," <u>Computerworld</u>, September 26, 1983.

[178] In other words, the government doesn't have to prove that the act was done designedly, understandingly, knowingly, or with guilty knowledge.

record keeping, control and asset preservation."[179] And Robert Bigelow subsequently wrote that, since such records are probably on computers, management has an obligation to ensure that access controls and protective techniques are appropriate.[180]

That it was the SEC's intent to use the accounting provisions to back-stop the anti-bribery sections was made clear during the original congressional hearings by SEC Chairman Harold M. Williams,[181] as well as by the subsequent issuance by the SEC of an accounting release specifically informing companies, accountants, and attorneys of the law's requirements.[182] A 1985 paper dealing with the SEC's enforcement of the FCPA noted:

> The impact of the accounting, record keeping and internal control provisions of the FCPA has certainly gone well beyond the area of foreign and domestic payments. . . . Subsequent to the FCPA's enactment, the SEC's enforcement efforts have focused almost entirely on these provisions of the law.[183]

Initial views on the importance of the accounting provisions of the FCPA have proven to be correct.[184] From its passage until mid-1986, the SEC brought 73 actions to enforce the accounting requirements, including

---

[179] See note 160.

[180] See note 70 at 13.

[181] See note 175 at 46.

[182] See note 175 at 50.

[183] McLucas, William R., and Alexander T. Moore (both officials in the SEC's Division of Enforcement), "Update – Recent SEC Enforcement Activities Involving the Foreign Corrupt Practices Act and 'Cooked Books,' " paper prepared for the Eastern Regional Conference of the Institute of Internal Auditors, April 21-24, 1985, 1-2.

[184] Only about 4 percent of the SEC's enforcement actions have been based on the anti-bribery sections of the FCPA. Percentage derived from data in McLukas and Moore, see note 183 at 2.

65 injunctive suits and 8 administrative proceedings.[185] Although statistical data on the outcome of these cases is difficult to come by, the great majority clearly are settled; although the company does not admit guilt, it agrees to all or most of the injunctions requested by the SEC.[186]

The FCPA cases brought by the SEC point to the possibility that, as the essence of corporate accounting is increasingly embodied in automated information resources, the SEC might go after a company that failed to employ adequate security controls over those resources, to ensure the integrity of the SEC-required information.

In summary, statutes and regulations may have obvious and explicit, or hidden and vague, implications for corporate policy-making on the protection of information resources. Some of these, such as the record-keeping provisions in federal securities exchange law, will almost certainly increase in importance as more financial records are computerized, vulnerabilities are increasingly publicized, and protection is increasingly available – changing the standard of "reasonable" as applied under that law.

Thus far, this chapter has examined various approaches to estimating financial value as an indicator of the need to protect corporate information resources. Also, it has examined the issue of legal "value" from several perspectives: the adequacy of state and federal law to protect corporate information, considerations of corporate liability, and finally, statutory and regulatory requirements affecting the need to protect information resources. Although these elements are critical in the value-vulnerability approach to developing corporate policy for the protection of information resources, they are not the only considerations. Other factors are considered in the following section.

---

[185] "Witnesses at Senate Hearing Differ on Effects of Foreign Corrupt Practices Act Amendments," Bureau of National Affairs' Daily Report for Executives, June 11, 1986, A-2.

[186] This information is based on a telephone query to the SEC's Division of Enforcement, August 23, 1989.

3.3 OTHER FACTORS

In addition to the financial and legal considerations important in assessing the value of information resources, various other aspects may or may not be of significance, depending on intangibles such as overall corporate "philosophy" and "culture," or more concrete factors such as company size and degree of organizational hierarchy. Among them are psychological, organizational, and ethical considerations. In contrast to financial and legal considerations, which have a certain external discipline attached to them by the markets and the courts, the psychological, organizational, and ethical implications of corporate policy for the protection of information resources are largely "softer" concerns which reflect the internal personality of the corporation and its management. These three "soft" aspects also differ from financial and legal considerations in that they are not as individually separable; questions of financial and legal value can almost always be separately addressed, whereas questions of ethics, for example, frequently blend into questions of organization and psychology.

It is understood, of course, that any important business decision will be considered carefully from a variety of perspectives. The discussion which follows is intended to identify considerations that have particular pertinence to information resources policy.

3.3.1 Psychological Considerations

In developing corporate policy for the protection of information resources, it may be useful to ask questions about the possible psychological impacts – intended and accidental – such a policy may have on employees, shareholders, and others who have a stake in the corporation's activity. Although some may dismiss the importance, or even the reality, of a psychological dimension to such decisions, it nevertheless appears to be true that such corporate actions send real messages to stakeholders which can be of long-term importance.

For example, if a corporation does not have a policy on the protection of information, or if it has a policy that suggests

protection is in the category of a back-burner afterthought, common sense and common observation indicate that employees will tend to pick up on this "message" and treat security of information as a low priority – something to wink at. This psychological mechanism was vividly illustrated in the case of Christopher Boyce, who began his career spying for the Soviets in a corporate environment which, underneath all the security regulations, did not treat the regulations or their violation as serious matters. After his arrest, Boyce explicitly acknowledged the psychological messages he picked up suggesting corporate laxity.[187]

The following questions, then, should be considered when management makes a decision affecting the protection of corporate information resources:

- How will employees, managers, shareholders, customers and clients, regulators, and prospective employees and managers perceive this decision with respect to the company's commitment to security, the importance of confidentiality, the peace of mind about information that particular stakeholders consider sensitive, and so on?

- Does the psychological message sent have a "good guy/bad guy" or a "hard line/soft line" dimension to it? If so, is this consistent with other such messages from management? Should it be hardened or softened?

- What part does sending intentional psychological signals play in this decision? How important is the psychological signal in the basic decision being made?

- What <u>is</u> the intended signal, if there is one? Can it be simply stated?

- At whom is the psychological dimension of the action aimed?

- Is the timing critical? How will this message be seen within the context of recent events? Does it have a "knee-jerk" reaction, or a forward-looking component?

- Does the management level that originates the action play an important role in its likely psychological meaning?

---

[187] Lindsey, Robert, <u>The Falcon and the Snowman</u> (New York: Simon & Schuster, 1979).

- Is there an "autocratic/democratic" dimension to the message being sent? Would broader or narrower participation in the decision or action change the nature or degree of this dimension?

- How likely is it that the psychological message will be misinterpreted? Is there anything that can be done to make it clearer?

- How much does the action or decision emphasize the issue at hand? Does it over-emphasize a management concern in the eyes of employees, managers, and so on? Does it contribute to an atmosphere of everything-is-top-priority?

- What message is sent to individual employees (or others) concerning their sense of pride, security, fear, confidence, and loyalty towards the corporation?

Not meant to be all-inclusive, these questions are offered as examples of the kinds of questions which, when considered, might prevent the psychological dimensions of security policies from falling between the cracks of debates dominated by financial and legal factors.

Some of these concerns were reflected by Hans Von Braun, corporate security manager with the Palo Alto, California, branch of Hewlett-Packard: When a security breach is committed "we deal with it harshly and swiftly . . . a breach of trust is a serious offense at our company." To instill company loyalty among its employees, he said, the organization promotes sharing of information and decision making among all levels of management. "When employees in a work group decide that they need a LAN," he explained, "they form a committee to determine what security will be necessary."[188]

The suggestion here is to at least consider the potential psychological dimension of security policies. In some cases it may be an obvious factor (or even the reason for the policy). In other cases it may entirely escape notice without deliberate and focused consideration.

---

[188] Mason, Janet, "The Secret to LAN Security," PC Week 5, no. 15, (April 12, 1988), S18.

3.3.2 Organizational Considerations

In a similar manner, it may be useful to ask specific questions about the organizational impacts of corporate policies for the protection of information resources. Many such policies directly affect the flow of information within an organization, often dealing with the question of access: Who does/does not have access to particular information, and who controls this access? Some questions to consider are listed below:

- Does this action or decision generally increase or decrease access to information? Which information? Access by whom?
- How important is access to or control over this information resource to the operational performance of different organizational elements? To the corporation as a whole?
- Does this action somehow shift control over the information resource? Who gains more control? Who loses control? How does this shift affect organizational power relationships?
- What does this decision do to management access to the information resource?
- What about personalities and "turf"? How will key individuals view and respond to the policy? Is someone being intentionally or unintentionally upgraded or downgraded?
- Are the effects on organizations/personalities/turf/access consistent with other management actions? If not, is this intentional?
- What are the implications for organizational resources? How does the decision affect workloads and requirements for office space, equipment and supplies, and personnel?
- What are the likely impacts on future employee expectations? Will career paths be newly created and expanded, limited, or even eliminated?
- How reversible or manageable are likely organizational impacts once the policy is implemented?

Again, these questions are not exhaustive. Rather, these examples suggest the kinds of organizational impacts potentially caused by corporate policies for the protection of information resources.

3.3.3 Ethical Considerations

"Ethics," as a matter of corporate and public policy, has recently become a highly visible issue. As Jay BloomBecker notes: "In 1989 'ethics' is appearing as a word in the newspapers more than [it did in] 1984. . . . Society tends to fret more about ethics these days."[189] When publicly discussed, however, ethics – and especially "business ethics" – are treated as a joke (literally, as in "Business Ethics: The Shortest Book in the World"). Or, they are sharply focused on specific scandals, such as illegal trading on Wall Street, or on major corporate issues and events, such as plant location or relocation, plant safety, corporate takeovers and buyouts, responsibility for toxic waste dumps, oil spills, plane crashes, and poison gas leaks. One does not often read or hear about the ethical dimensions of corporate use and misuse of information resources except, perhaps, when an especially serious lapse involves personal information and privacy. Yet, in many ways "ethics" of one sort or another have a bearing on the overall subject of corporate policy for the protection of information resources. Some of these are listed below:

- The issue of privacy for personal information, and its relationship to pre-employment screening, and employee testing and monitoring
- The impact of higher technology on ethical behavior, for example, ethical changes associated with the depersonalization of certain technological applications
- The possibly unusual ethical standards of specific groups, such as computer "hackers" and computer criminals
- The education – or lack of education – in our schools and universities concerning the ethical aspects of technology and its use
- The value of corporate ethical codes and policies, or of published codes of behavior
- The basic question of ethics and corporations: Can a corporation, as opposed to an individual, be understood to have a "conscience?"

---

[189] BloomBecker interview.

- The relative ethical roles of the market, the government, and corporate management

A comprehensive discussion of these ethical aspects and their relationship to information resources policy is certainly beyond the scope of this report. However, a few questions concerning the ethical obligations of a corporation are worthy of examination here for several reasons. First, Sissela Bok argues that

> powerful new techniques of storing and of probing secrets increase the need for careful debate. From the miniature camera . . . to the methods of securing and invading computerized information banks, new means beckon to anyone who would abuse either openness or secrecy.[190]

A second reason is that decisions regarding information resources can have serious effects on individual lives. James O'Toole maintains that "decisions people make in business have an impact on other people's lives, and as soon as they have that impact, they take on an ethical dimension."[191]

To the extent that a corporation desires to examine the ethical aspects of its information resources policy, there are several general frameworks for such an examination which lean more towards the practical than the philosophical. Two qualities that have been suggested as necessary for ethical corporate policies, for example, are rationality and respect.[192] Kenneth Goodpaster and John Matthews describe "rationality" as follows: "Taking a moral point of view includes the

---

[190] Bok, Sissela, Secrets: On the Ethics of Concealment and Revelation (New York: Random House, 1983), xvii.

[191] Interview with James O'Toole, quoted in Inc., January, 1986, 29.

[192] See: Goodpaster, Kenneth E., and John B. Matthews, Jr., "Can a Corporation Have a Conscience?" Harvard Business Review, January-February 1982, 134. They also offer an interesting discussion on competing views of who is, or should be, responsible for corporate ethical behavior – i.e., "the invisible hand" of the market, the hand of government, or the hand of management.

features we usually attribute to rational decision making, that is, lack of impulsiveness, care in mapping out alternatives and consequences, clarity about goals and purposes, attention to details of implementation." They discuss "respect" as follows: "The moral point of view also includes a special awareness of and concern for the effects of one's decisions and policies on others. . . . This is respect for the lives of others and involves taking their needs and interests seriously, not simply as resources in one's own decision making . . . not merely as a useful precaution (as in 'honesty is the best policy') but as important in its own right."[193]

In addition to questioning the ethics of a policy by its rationality and respect, as outlined above, Laura Nash suggests twelve questions useful in examining the ethics of a business decision.[194] Five appear to apply directly to decisions on the protection of information resources:

- What is your intention in making this decision?
- How does this intention compare with the probable results?
- Who could your decision or action injure?
- Can you discuss the problem with the affected parties before you make your decision?
- What is the symbolic potential of your action if understood? If misunderstood?

An area of special ethical sensitivity, with respect to corporate policies on the protection of information resources, involves the private and personal information that corporations increasingly collect

---

[193] Ibid.

[194] Nash, Laura L., "Ethics Without the Sermon," Harvard Business Review, November/December 1981, 81-90.

and maintain on their prospective, current, and ex-employees.[195] Particular concerns center on questions such as

- Is this information needed?
- Is it accurate?
- Is it up-to-date?
- Who has access to it?
- If this information is passed along to another party, what continuing controls exist to ensure its accuracy and limit access to it?

These questions apparently are becoming more and more important as corporations – hit by absenteeism, theft, high turnover, rising insurance and medical costs, and potential liability for the actions of impaired employees – increasingly scrutinize employees' historical records, attitudes and honesty, physical and mental health, and personal habits. Employee drug testing has greatly increased,[196] and Meredith Mendes notes that

> testing for AIDS is especially problematic. Most of the tests offered have high rates of both false positives and [false negatives] – traumatic enough in drug testing but particularly so with AIDS. . . . Yet so far, only California has acted to prohibit AIDS testing as a condition of employment.[197]

Clearly, corporations have an ethical burden to ensure the accuracy of any such data which it may collect and maintain, and to protect

---

[195] For an in-depth discussion of the importance of personal privacy to personal identity, see: note 190, Bok. For a variety of views on corporate ethics and technology, see: Whieldon, David, "Ethics Roundtable," in Computer & Communications Decisions vol. 16 (October 1984), 92. For an overview of personnel files and privacy, see: Solomon, Jolie, "As Firms' Personnel Files Grow, Worker Privacy Falls," Wall Street Journal, April 19, 1989, B1.

[196] See note 128; and Marx, Gary T., and Sanford Sherizen, "Monitoring on the Job," Technology Review, vol. 89, November 1986, 62.

[197] Dentzer, Susan et al., "Can You Pass the Job Test?" Newsweek, May 5, 1986, 46.

against any improper disclosure of the results of such tests – or of employee monitoring and other personal data. This responsibility is likely to grow as technology offers new kinds of personal information about people, such as genetic testing for disease, behavior, or personality "markers." To the extent that such personal data is increasingly maintained in automated information resources such as computers, computer systems, and networks, the ethical dimensions of the protection of these resources can be expected to grow.

Guidelines for the protection of personal information, drawn up in 1973 by the Department of Health, Education and Welfare's Advisory Committee on Automated Personnel Data Systems, may offer a basis for the ethical treatment of such files in the corporate environment:

1) There must be no personal data record-keeping systems whose very existence is secret;

2) There must be a way for an individual to find out what information about him is in a record and how it is used;

3) There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent;

4) There must be a way for an individual to correct or amend a record of identifiable information about him; and

5) Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for its intended use and must take reasonable precautions to prevent misuse of the data.[198]

Because modern information resources within corporations are rapidly changing, special attention may be called for in conducting periodic reviews of those resources which might contain or process sensitive personal data. Another policy consideration deals with the question of published corporate codes of ethics, insofar as they address the use of information resources.

---

[198] See note 81 at 209.

Perhaps the main question that needs to be raised is whether codes of ethics are effective in promoting more ethical behavior in an organization. On the "pro" side, Harry B. DeMaio writes that "with information . . . our inclination is to communicate and share. In the absence of explicit instructions, we often 'forget' confidentiality and give in to the urge to communicate."[199]

In this view, explicit codes offer clear guidelines, reminding people of the things they should do, but might not think about in the normal course of events. They also make it difficult for people to claim after-the-fact that they didn't realize a particular action was prohibited, something which can be useful in subsequent disciplinary action. They may also encourage some people, who might otherwise hesitate, to act on specified ethical practices:

> One advantage of a code is that it allows timid employees to do the right thing. If they're pressured to compromise standards, they can say, "I'd like to, but I can't. The company has a code that doesn't allow us to do that."[200]

On the other hand, some maintain that

> codes of conduct may actually do more harm than good. Ethical codes are necessarily minimal; they formulate the least that needs to be done. This may incline professionals to not do their best but do just what the code requires. Perhaps worse, codes of conduct can stifle the dissenter, the critic, or the creative person and degenerate into that situation John Stuart Mill called the "tyranny of the majority."[201]

It may be that the negative view prevails, or that the issue simply hasn't come up that often, as August Bequai quotes estimates that only

---

[199] DeMaio, Harry B., "The Information Ethics Issue: It's Time for Management Action," Datamation, Computer Security - Issues and Trends, 1988.

[200] Robert Ellis Smith, quoted in David Whieldon, "Ethics Roundtable" (see note 195).

[201] Czarnik, Stan, book review of Ethical Issues in the Use of Computers, by Deborah G. Johnson, in Byte, December 1985, 72.

10 to 22 percent of companies have written guidelines dealing with the ethical use of computers.[202]

Another view is that it is not the corporate policy per se which is of value, but rather the process involved in developing one, which forces a company to think about, discuss, and confront its ethical priorities.[203] Jay BloomBecker believes that ethics codes are important and useful, but that the process of establishing one is more important than the code itself.[204] Taking a more personal view of the need for ethical codes, Harry B. DeMaio sums up:

> Developing a code of conduct is a slow, uncomfortable process. It won't contribute directly to the bottom line – in fact, it will involve added expense. Yet, as individuals and institutions, we must wrestle with our own consciences and state explicitly – to employees, students, customers, vendors, associates, and collaborators – what our ethical expectations are and how we expect them to be observed.[205]

This section has examined five elements that contribute to a broad concept of value for corporate information resources: financial, legal, psychological, organizational, and ethical. The need to protect information resources partially depends on the emphasis a corporation places on its own interpretation of these considerations. The other element necessary to determine the need for effective protection policies is an understanding of the vulnerability of those information resources deemed to be valuable.

---

[202] See note 35, Bequai.

[203] See note 194 at 88-89.

[204] BloomBecker interview.

[205] See note 199.

CHAPTER FOUR

VULNERABILITY

This chapter addresses the possible threats to and susceptibilities of information resources. It provides a checklist of threats and susceptibilities – with concrete examples – which may be considered in determining the need to protect information resources.

Vulnerability is defined here as a combination of 1) threats that act to cause damage, and 2) susceptibilities to actions that allow such damage to occur. Threats to information resources fall into three categories: chance events, non-hostile human agents, and hostile human agents. Susceptibility involves an openness to actions such as intrusion, deception, theft, disruption, interception, destruction, and data alteration. For damage to occur, both elements are required – an actor to cause damage, and a susceptibility to being damaged. Corporate actions to protect information resources may be aimed at either or both elements of vulnerability.

4.1 THREATS

4.1.1 Chance Events

Chance events that can damage corporate information resources range from relatively commonplace incidents, such as fires and storms, to extremely rare accidents, such as volcanic eruptions. Such threats are listed below, in a very rough order of their likelihood:

- Fires
- Storms (including tornadoes and hurricanes)
- Power outages or disruptions
- Water leakage or seepage (from fire damage, condensation, broken water pipes, and the like)
- Floods
- Lightning

- Gas leaks
- Earthquakes
- Volcanoes
- Geo-magnetic storms (including solar storms and flares)
- Toxic spills
- Accidents involving automobiles, trucks, and animals
- Nuclear reactor accidents
- Plane crashes or falling debris
- Meteors
- Spacecraft debris
- Accidents, disease epidemics, and so on involving key personnel

Although fires are the biggest threat, information resources such as data processing centers have been knocked out by unusual and freak events. Major communications links have on occasion been severed by freak accidents such as cables being cut by digging machines or farm equipment.[206] Electrical shorts even have been caused by animals chewing on wires or crawling into equipment.

Animals cause more damage than is widely known. On May 11, 1989, a raccoon managed to electrocute itself at the University of Utah, causing a 20-second power outage that caused the loss of data on computers being used to verify recent cold fusion experiments.[207] Peter Scott of NASA's Jet Propulsion Laboratory (JPL) notes that raccoons have crippled JPL on

---

[206] During the author's active military duty at Naval Communications Station, Spain, the primary east-west naval communications link was knocked out for six hours by a farmer's plow.

[207] Reported on the National Computer Security Center's DOCKMASTER network RISKS form, this story was contributed by Peter Scott on June 1, 1989. The story originally appeared in Science News.

more than one occasion, and similar incidents involving squirrels, birds, rabbits, and so on[208] have been reported by other organizations.

Acts of nature are another source of damage to information resources. In the 1980 explosive eruption of Mt. St. Helens, the volcanic ash injected into the atmosphere caused damage to sensitive computer disks and disk drive mechanisms.[209]

And on March 13, 1989, the largest magnetic storm in forty years took place. The rapid changes in the geomagnetic field induced voltages in power lines, ocean cables, and cable and TV networks. In Quebec, the storm caused the failure of power transformers which blacked out large areas, and the space shuttle "Discovery" was recalled a day earlier owing to computer malfunctions which may have been caused by the magnetic storm.[210]

Among the more likely chance events is water damage to hardware, software, and information media. Approximately 35 percent of all data center insurance claims relate to water damage.[211] The water usually comes from broken pipes, plugged drains, roof leaks, ground water seepage, floods, and accidental discharge of fire extinguishers or sprinkler systems.

But fires are by far the most frequent and most damaging of the chance event threats. Over 160,000 New York Telephone subscribers were denied service by a 1975 fire that damaged local and tandem switching

---

[208] Reported on the National Computer Security Center's DOCKMASTER network RISKS form, these stories were contributed by Peter Scott et al.

[209] Computer Security (Alexandria, Va.: Time-Life Books), 33.

[210] "The Geomagnetic Storm of 13 March 1989," Radio Communication 65, no. 5 (May 5, 1989).

[211] Rothstein, Philip J., "Up and Running: How to," Datamation, October 15, 1988, 86.

equipment in Manhattan.[212] And in 1987, 41,000 Brooklyn customers lost telephone service for three weeks after a central office fire.[213] But the Hinsdale, Ill., fire (briefly discussed in chapters 1 and 3) has been called "the worst telecommunications disaster in U.S. telephone industry history."[214]

In addition to the serious damage the fire caused, its causes and its implications for other central offices and other types of information resource facilities illustrate the persistent and pervasive nature of random threats (not to mention Murphy's Law). In the wake of the Hinsdale fire, initial discussion focused on how damage might have been limited by faster alarm responses, or the use of sophisticated fire suppression equipment, such as Halon gas extinguishers.[215]

However, a March 10, 1989, report by the Illinois Commerce Commission, which carefully investigated the incident, concluded otherwise.[216] The Hinsdale central office switch was equipped with ionization smoke detectors and special detectors in areas such as the diesel generator room (there were two generators for backup power, as well as DC power backups). The fire and communications alarms were remotely monitored in Springfield, Ill. The Springfield center started receiving alarms as thunderstorms moved through the Hinsdale area, disrupting commercial power.

---

[212] IEEE Spectrum, June 1975, 34, noted in: Block, Ellen G., and Henry D. Levine, "Protecting the Last Mile: The Quest for a Robust Local Exchange Network," Telematics 5, no. 10 (October 1988), 12.

[213] The New York Times, March 1, 1987, 41; noted in Block (see note 212 at 12).

[214] Wilson, Carol, "Hinsdale's Aftermath: COs at Risk," Telephony, March 20, 1989, 21.

[215] Karwath, Rob and Christine Winter, "Phone Repairs to Run into June," Chicago Tribune, May 13, 1988, 1.

[216] The following discussion is based on Carol Wilson's "Hinsdale Aftermath: COs at Risk" (see note 214).

The first two sets of alarms indicated commercial, and then diesel, power failures. These power alarms were accompanied by fire alarms, but the fire alarms cleared as each backup power system was activated. Because of these power alarms, a separate fire alarm was interpreted by the Springfield operator as part of the power problem, rather than as a fire. The result was a 40-minute delay before the fire was discovered by a central office technician who, being dispatched to the scene, tried to call the fire department. By that time, however, local telephone service was disrupted, so the technician alerted a passing motorist, who alerted police, who finally alerted the fire department.

The fire had started in cable racks suspended from a 14-foot-high ceiling. A damaged DC power cable in the overhead rack had come into contact with an armored cable, throwing out a spark. The older insulation on one cable provided the initial fuel for the fire, which burned very hot from the outset, igniting a fire-retardant cable that released corrosive gases; it was the corrosive gas which did the real damage within the first twenty minutes.[217]

The Illinois Commerce Commission report noted that even if help had arrived sooner, the damage would have been done anyway. It was also reported that the use of Halon gas would not have helped; because Halon is heavier than air, it would not have extinguished the fire in the suspended racks. Similarly, water sprinklers would not have saved the switch, as they would have damaged the electrical equipment. The report concluded that a similar disaster could occur, given a similar sequence of events, at any of the hundreds of central office switches scattered around the country which are built to the same standards and specifications.

From the perspective of companies that rely on information resources, such as the public telephone network, several lessons can be drawn from the Hinsdale fire. First, corporations can never be certain that <u>all</u>

---

[217] Wilson, Carol, "Cable Issues Still Burning after Hinsdale," <u>Telephony</u>, April 17, 1989, 13-14.

contingencies are addressed by their own emergency or disaster recovery plans. Many companies hurt by the fire had elaborate business continuity plans which, nevertheless, did not anticipate the possibility of a major commercial telephone failure. And second, corporations can never be certain that their technical or procedural precautions for ensuring the operation of internal information resources will be effective against all possible circumstances. These uncertainties have important implications for the mix of protective measures which should be considered, and are discussed in chapter five.

4.1.2 Non-Hostile Human Agents

Non-hostile human agents, that is, individuals who do not intend harm to a particular victim, come in many varieties. A checklist of such threats would include people who are

- Careless, ill-trained, or incompetent
- Mentally deranged
- Drug or alcohol impaired
- Hostile to someone else, but who harm unintended victims

Some would argue that these threats are greater than those presented by deliberately hostile individuals. Patricia Keefe, for example, refers to a group described as "the ignorant:"

> This group includes any user who accidentally wanders into the wrong files, unintentionally deletes or writes over information or creates any kind of error likely to result in downtime and expensive, corrective measures. This type of breach makes up the bulk of security problems.[218]

Robert Bigelow agrees: "The greatest threat to computer security is the unintentional act of an employee who is well meaning but negligent

---

[218] Keefe, Patricia, "It can't happen here...," Computerworld, April 6, 1988, 13.

or poorly trained."[219] And computer consultant Robert Courtney has conducted surveys which suggest that as much as 65 percent of company dollar losses can be attributed to unintentional mistakes made by employees.[220]

In one incident of this type, the high-tech Framingham suburb of Boston lost telephone service for one day when technicians accidentally blew two 600-amp fuses in a central office switch during routine maintenance.[221] In a different kind of incident, an employee of a Minnesota company intended to FAX a strictly confidential corporate top secret document dealing with a proposed acquisition to one of its major shareholders. A new employee made a mistake, however, and transmitted the secret plans to the Chicago news bureau of the Wall Street Journal.[222]

Myriad incidents also have occurred because of computer programming errors, poor operating instructions, or carelessness in the use of computer systems. Commercial loans in California were brought to a near standstill by a computer system designed to perform the equivalent of a title search for commercial borrowers, causing a backlog of 50,000 requests.[223]

Software errors and sloppy de-bugging are attributed with causing banks to lose up to $650 million in student loans. In this case, the

---

[219] See note 70 at 10-19.

[220] Fitzgerald, Karen, "The Quest for Intruder-Proof Computer Systems," IEEE Spectrum, August 1989, 22.

[221] Network World, July 11, 1988, 1; noted in Block & Levine, note 212.

[222] Kotlowitz, Alex, "Believe Us: This Isn't the Way We Break Most of Our Stories," Wall Street Journal, December 19, 1988, B1.

[223] Reported by Peter G. Neumann, based on a June 14, 1989, article by Kenneth Howe in the San Francisco Chronicle.

software caused payments from overdue borrowers to be rejected, and incorrectly addressed collection notices.[224]

In one of the largest, most carefully designed and protected corporate information resources – American Airline's SABRE passenger reservation system – an improperly tested software addition cost the company as much as $50 million. The errors caused the system to indicate that planes were sold out of certain fare classes when, in fact, they were still available. After telling the customers that no tickets were available, the system referred them to competitors.[225]

A special class of non-hostile threats includes those who may have hostile intent towards someone else, or perhaps towards no one in particular. For example, a computer "virus"[226] created by a programmer who intends to "infect" a particular target system may unintentionally infect many other systems. Such viruses, as well as similar programs are known as "worms."[227] There are many examples of this happening in what at least one observer has called "The Viral Age."[228] The Providence, Rhode Island, Journal-Bulletin computer center was hit by a virus that erased important files. This particular virus, known as the "Pakistani Brain" virus, had been designed over two years earlier by a young programmer from Punjab province. In its original version it did not erase files, but it was later modified by a second programmer.

---

[224] McCoy, Charles F., and Richard B. Schmitt, "United Education's Computer Blunders Form Vortex of Big Student Loan Fiasco," Wall Street Journal, March 10, 1989, A6.

[225] Andrews, Nina, New York Times, September 12, 1988.

[226] A "virus" is a computer program, usually destructive or annoying in nature, that attacks, enters, and embeds itself into a legitimate program, and may replicate itself indefinitely. It may be transmitted over a network, or spread from one computer disk to another by way of a common machine.

[227] A computer "worm" is similar to a virus, but exists as an independent program: it doesn't embed itself into another program. The so-called "Internet Virus" of November 1988 was in reality a worm program.

[228] Hodges, Parker, "Opinion," Datamation, December 1, 1988, 96.

Neither programmer had any hostile intent specifically targeted at the Journal-Bulletin.[229]

University of Cincinnati computer expert, Frederick Cohen, suggests the scale of the computer virus threat:

> In just six months, beginning in September of 1987, about 100,000 computer systems sustained some form of damage from computer viruses. Microcomputers, mainframes, engineering workstations, and worldwide computer networks have all been affected. Viruses have hit every major computer manufacturer, and they have even begun to enter commercial software distribution channels. Over 10,000 legitimate software packages from major software manufacturers have been distributed with viruses in them, and viruses have even been found in beta test software delivered to distributors.[230]

Some estimates of the number of viruses in existence are higher, others are lower, but nearly all observers and experts agree that the threat is very high – and growing. Although many of these viruses and worms are created with hostile intent, many others are not. Twenty-three-year-old Drew Davidson, who authored the so-called "Peace" virus,[231] did so at least partially to show off his programming skills: "In the beginning I didn't think it would have this kind of impact. . . . I just thought we'd release it and it would be kind of neat."[232]

These and many other similar incidents suggest that, in developing corporate policies for the protection of information resources, the wide

---

[229] Hafner, Katherine M. et al., "Is Your Computer Secure?" Business Week, August 1, 1988, 64; also, see note 36, Elmer-DeWitt at 62.

[230] Cohen, Frederick B., "Computer Viruses: A Contemporary Affliction," Datamation, Computer Security Issues and Trends, September, 1988.

[231] This was the first known example of a virus spreading to a commercial software package, Aldus' "Freehand" graphics program for Macintosh PCs.

[232] See note 36, Elmer-Dewitt at 63.

variety of threats from non-hostile human agents must be given careful consideration.

4.1.3 Hostile Human Agents

A different kind of threat, and in many ways the most dangerous, is presented by human agents who have hostile intent towards a corporation. Hostile agents may be corporate insiders, such as employees, consultants, and contractors, or they may be outsiders, such as ex-employees, terrorists, computer hackers, criminals, rioters and strikers, or competitors.

Perhaps the single biggest threat is the trusted insider who, by virtue of his access to and knowledge of the company's information resources, may be able to do extraordinary damage, and may be especially hard to detect. For the top management of the Centel Corporation of Chicago, the hostile insider is clearly the biggest worry. The company believes that accidental damage is largely addressed by routines, controls, and procedures, but that the hostile insider is the most difficult to protect against.[233] According to Ray Huffmaster, owner and operator of the private investigation firm, Huffmaster Associates of Dearborn, theft is more of an internal threat:

> You get into big industry, you're talking about millions and millions of dollars for industrial espionage. It's a fantastic threat. For example, you've got a salesman who has gone bad – he's defected to another company. Every time the company bids on widgets, they're off by one cent. . . . We get called in for a lot of that. They think first "Our phones are tapped." Nine times out of ten, that's not the case. It's a secretary giving someone the information over the phone; it's a salesman who may be getting paid by another company to get this information out.[234]

---

[233] Eugene Irminger, CFO, and Richard Kokoszka, director, Internal Auditing, interview with author, May 23, 1989.

[234] Huffmaster, Ray, quoted in an interview with Philip Ginotti, "Private Eye," Oakland Business Monthly, May 1988, 56.

Common motivations for insiders to turn against their own employers include

- Personal gain and wealth
- Entertainment
- Revenge
- Personal favor
- Ambition
- Challenge of beating "the system"
- Jealousy
- Sheer destructiveness

But not all insider attacks on information systems are motivated by such understandable or rational reasons. Employees and other insiders have been known to act irrationally towards information resources, perhaps out of frustration or uncontrollable anger. Computer systems, for example, have been attacked with screwdrivers, beaten with shoes, thrown from windows, and shot at with pistols. In one case, a woman received five years in prison and a $500,000 fine for "pounding to death" a computer at Vandenberg Air Force Base; she seemed to think the computer was part of a "first-strike nuclear force."[235] In expressing perhaps the ultimate human threat to a delicate machine, an unidentified insider in the office of the U.S. Solicitor General once urinated on a computer, rendering it inoperable![236]

Other, more rational, actions may have similarly unusual origins. Boredom on slow midnight work shifts has led some individuals to damage an information system, simply to generate excitement and attention. For example, at a large remote processing service bureau owned by Dun & Bradstreet, a technician planted a "logic bomb" – a hidden piece of computer code, which can be programmed into a computer with instructions

---

[235] See note 70 at 10.

[236] See note 209 at 42.

to be activated on a certain date or under certain circumstances – in the programs governing a west coast computer system. His motivation? To be sent cross-country to repair the "problem," obtaining a free trip to California just before his vacation started.[237]

Other employees have taken steps to ensure what might be called "anticipatory revenge." Several incidents have been reported where computer programmers placed logic bombs into company payroll programs that either reduced or raised employee paychecks. These bombs were set to go off six months after the programmers' names disappeared from the employee list.[238]

Perhaps with a sense of misplaced idealism, a group of "high-tech Robin Hoods – possibly including employees of Apple Computer, Inc." – seem to be trying to disseminate the closely held source code for Apple's Macintosh computer. A letter signed by an individual or group calling itself "the New Prometheus League (Software Artists for Information Dissemination)" declared:

> Our objective at Apple is to distribute everything that prevents other manufacturers from creating legal copies of the Macintosh. . . . As an organization the New Prometheus League has no ambition beyond seeing the genius of a few Apple employees benefit the entire world.[239]

Although revenge, jealousy, idealism, and craziness have all contributed to insider threats against corporate information resources, the primary motivation remains in that familiar realm of everyday, garden-variety greed. Theft of one sort or another continues to be the primary offense, whether it is theft of, or theft by, information resources. Objects of or tools in such theft may be information,

---

[237] See note 38.

[238] Ibid.

[239] Lowenstein, Roger, and G. Paschal Zachary, "Mysterious Group Is Pirating Apple's Super-Secret Code," Wall Street Journal, June 8, 1989, B7.

communications and computer hardware, software, access control codes and passwords, computer or network time and services, or supplies. Examples of such theft abound, even though it is generally believed that most cases go unreported outside of the victimized organization. A few cases that illustrate the scale of losses, and the range of insider scams, include the following:

- The $21.3 million Wells Fargo Bank loss (noted in chapter 3) was caused by computer fraud by an officer of the bank. Similarly, Stanly Mark Rifkin was a computer consultant for Security Pacific National Bank when he stole $10.2 million by way of a fraudulent wire transfer.

- A computer programmer at a Los Angeles bank illegally diverted about $10,000 to his own account to help support his wife's drug habit.[240] He was eventually caught by a random audit.

- A lawsuit and indictment have been filed against two individuals who allegedly stole more than 50 million "frequent flier" mileage awards, which were then sold for cash. The scam involved entering American Airlines' reservation system, and then shifting credits for unclaimed mileage flown by passengers who were not enrolled in the airline's frequent-flier program. Access to the system was easily obtained by one of the pair, as she was an employee of a local (Tulsa, Okla.) travel agency.[241]

- National Bonded Money Co., a Shreveport, La., firm, sustained losses of $141,000, and had to be sold by the family that owned it. The losses were caused by a computer "trojan horse,"[242] which stole money orders at the rate of about $1,000 a day. The culprit, who was sentenced to seven years' hard labor in prison, was a programmer working as a consultant in upgrading the company's main processing program.[243]

---

[240] See note 40.

[241] Dahl, Jonathan, "Racking Up Mileage: The Easy Way," Wall Street Journal, November 4, 1988, B1.

[242] A "trojan horse" is a program that appears to serve a useful and legitimate function, but which contains within it some unrelated code, usually having malevolent purposes.

[243] See note 38.

Lawrence Wills, of IBM, emphasizes the seriousness of the internal threat: "The real problem is errors, omissions, or well-thought-out acts by individuals who have authorized access to data."[244]

An equally dangerous threat is posed by ex-employees, especially those who have been fired. Donald Gene Burleson, for example, planted a program that erased sales commission records – for which he was convicted of a criminal violation in Texas – two days after he was fired.[245]

In late 1987 the Wollongong Group, a software company in Palo Alto, Calif., fired one of its customer support representatives. Two months later the company discovered that someone was logging onto its computers late at night, using a remote terminal and modem. After tracing the calls, the police raided the ex-employee's home and confiscated her personal computer and disks that contained millions of dollars worth of Wollongong proprietary software. Although the company invalidated her access code when she was fired, she apparently had obtained that of another employee.[246]

Hostile human threats to information resources are, obviously, not limited to corporate insiders or ex-insiders. Networked information systems are frequently targets for outside individuals who may be driven by any of the motivations that animate insiders.

For example, revenge was clearly the motive in the case of Richard Sandza, a Newsweek reporter, who wrote an article about computer hackers. After his article appeared, Sandza's life was threatened, and he was put on a "teletrial" on a Gainsville, Tex., electronic bulletin board called "Dragonfire." What really bothered him, however, was when hackers obtained his credit reports by rifling the files of the TRW

---

[244] See note 78.

[245] Ibid.

[246] Ibid.

credit information system. His Visa charge card number was also obtained and placed on a Charleston, W. Va., bulletin board called "Pirate 80."[247]

The political objectives of terrorist groups have also led to the destruction of information resources, even if they are not the primary, or only, target of attack. In 1970, for example, a radical anti-war group exploded a bomb at the Army Mathematics Research Center at the University of Wisconsin. In addition to (apparently unintentionally) killing a graduate student who was working late, the destruction caused $18 million damage to the building, its computers, and its data.[248]

In another case a computer hacker, apparently motivated by a desire to have fun, reprogrammed Southern Bell switching equipment, causing overflow calls to a Delray Beach, Fla., probation office to be routed to a New York sex talk line.[249]

Business competitors are not always above unauthorized use and abuse of their competition's information resources. In Florida, two former employees of a Tampa television station (Channel 13) were charged with a criminal violation of stealing information by tapping into the computer of a competing station (Channel 10). The two Channel 10 employees are accused of using their knowledge of rival Channel 13's news computer to enter the system to see what news stories Channel 13 was working on. Some break-ins were made shortly before news broadcasts in an apparent effort to avoid "scoops" by Channel 13. Until recently Channel 13 had ranked consistently as number one in the Tampa television news market. Its ratings have been slipping, however, permitting gains by its competitors, including Channel 10.[250]

---

[247] Ryckman, Lisa Levitt, "Hackers Take Revenge on Writer," AP, December 4, 1984, AM cycle, Domestic News section.

[248] See note 209 at 35.

[249] Baltimore Sun, June 13, 1989.

[250] "Two Accused of Computer Crimes in TV Rivalry," New York Times, May 11, 1989, A21.

Interest in competitor intelligence has clearly been growing in highly competitive industries. As one indicator, National membership in the Society of Competitor Intelligence Professionals has grown from 9 to 720 in three years, according to Roberta Brody, the organization's president.[251] Such groups, however, eschew illegal or unethical collection of information.

A major threat to a company's information resources by hostile outsiders continues to be the computer "hacker" – a lineal descendant of the "phone phreaks" of the 1960s and 1970s, who devised ways to penetrate and manipulate commercial telephone systems. To understand their prowess, one need only consider "Captain Crunch," the most famous of the phreaks. He took his unusual name from a breakfast cereal, every box of which contained a cheap toy whistle, which happened to produce a 2600 hertz[252] tone. When the whistle was sounded after dialing a long-distance number, the call was disconnected but the trunk line remained open without any further charges, so that further calls were free. According to Sherry Turkle

> his most mythologized "hack" became known as "the call around the world." Crunch sat in a room in California with two telephones. Using the whistle and his knowledge of international telephone circuitry and codes, he picked up the first phone and dialed the number of a second phone. The call started in California, went through Tokyo, India, Greece, Pretoria, London, New York, and back to California. The second phone rang. He talked into phone number one and heard himself twenty seconds later on phone number two.[253]

From tin whistles, increasing sophistication led to the development of "blue boxes," which could simulate various tones useful in

---

[251] " 'Competitor Intelligence': A Grapevine to Rivals' Secrets," Wall Street Journal, April 12, 1989, B2.

[252] This equals 2,600 cycles per second.

[253] Turkle, Sherry, The Second Self: Computers and the Human Spirit (New York: Simon and Schuster, 1984), 226.

manipulating the telephone system.[254] As computer terminals became increasingly available, the combination of programming skills and illicit mastery of the telephone networks led to the arrival of the modern computer hacker. Phone phreaking skills have continued to grow in sophistication, and continue to play a key role in many computer hacking strategies. One way to defeat a dial-back or call-back modem,[255] for example, is to reprogram the legitimate callback number for "call forwarding" to the hacker's number, so that the call-back modem makes the connection for the hacker (and, incidentally, charges the call to the host computer).

Hackers may be classified by a number of taxonomies, and the term itself has undergone significant changes over the years. A definition offered by (convicted) ex-hacker Bill "The Cracker" Landreth is probably as close as we can get to accepted current usage: "A person who often attempts to gain unauthorized access to large systems by using his personal computer equipment."[256] Landreth identifies five distinct types, based on their skill level and motivation:

1) Novice: Younger hackers (12 to 14 years old) who are out to play with the system

2) Student: More knowledgeable hackers, who are out to learn all they can

3) Tourist: Out for adventure

---

[254] Colchester, Nicholas, "Computer Kingdom Founded on Phreaks," London Financial Times, November 17, 1984, 19; and Langway, Lynn, and Jeff B. Copeland, "Telephones: Listening In," Newsweek, February 17, 1975, 79.

[255] This is a device that, when dialed up by a remote user, hangs up and then calls back the user's phone number, which is known to the system that is called. It is designed to reduce the likelihood of an unauthorized caller accessing a computer or communications system.

[256] Landreth, Bill, Out of the Inner Circle (Redmond, Wash.: Tempus Books, of the Microsoft Press, 1985), 26.

4) Crasher: Out to cause trouble, erase files, and so on

5) Thief: Out to steal (rarest type, often an insider)[257]

Others simply differentiate intruders as "Hackers" (the "Good Guys") and "Crackers" (the "Bad Guys").

Numerous articles have been written that examine the hacker "culture," the psychological profiles of hackers, and their value systems and personal ethics.[258] In general, these studies profile hackers (using Landreth's definition) as follows:

- Young (generally 8 to 21 years old)
- Male[259]
- Intelligent
- Having a meritocratic value system which holds skill and mastery in the highest regard, but holds property rights, privacy, authority, and similar traditional values in low regard.

These values were reflected in some of the elements of the hacker ethic outlined by Steven Levy:

---

[257] Ibid., 61-69.

[258] See, for example: Turkle, note 253 at 196-238; Weinstein, note 40; Coldwell, R.A., "Non-Professional Practices in Computing: Some Thoughts on the Next Decade or So," The Australian Computer Journal, November 1987, 215-18; Saffo, Paul, "Consensual Realities in Cyberspace," Communications of the ACM, June 1989, 664; Levy, Steven, Hackers: Heroes of the Computer Revolution (Garden City, N.Y.: Anchor Press/Doubleday, 1984), especially Chapter 2, "The Hacker Ethic"; Phillips, Kenneth L., "The Network Trespasser As a Human Being," Data Communications, December 1985, 272.

[259] However, hackers are not as exclusively young and male as some may think. Leslie Lynn Doucette, a 35-year-old female hacker, was recently indicted on a variety of federal telecommunications, computer and access device fraud laws. She faces up to 89 years in prison, a $69,000 fine, and restitution charges of up to $1.6 million. (Bushaus, Dawn, "Hacker Charged in Voice Mail Case," Telephony, July 10, 1989, 10.)

> Access to computers – and anything which might teach you something about the way the world works – should be unlimited and total.
>
> All information should be free.
>
> Mistrust authority – promote decentralization.
>
> Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race or position.[260]

Sherry Turkle suggests that, in this ethic, "the people who want to impose rules, the inhabitants of the 'real world,' are devalued, as is the 'straight' computer-science community."[261] Joan Fitzgerald believes that

> their attitude is, "If you let me into your system, it's your fault, not mine." They have no moral reservation about going in to a computer network or system and doing damage. They are still antiestablishment.[262]

So, in the case of hackers (in addition to the small number of outright thieves), there are these extra motivations, generally unrestrained by any respect for an owner's property rights over his information resource. That hackers represent a genuine hostile human agent threat to corporate information resources has been amply demonstrated by the documented cases of serious damage they have caused.

In one case, federal officials arrested one adult and smashed a computer intrusion ring largely made up of teenagers who had infiltrated the computer systems of more than twenty companies, including the Michigan Department of Treasury and Home Box Office cable TV. The

---

[260] See note 258, Levy at 27-30.

[261] See note 253 at 213.

[262] Fitzgerald, Joan, and Geoff Brouillette, "Protecting Against Loss Requires Deviousness, Skepticism," American Banker, February 10, 1984, 13.

estimated fraud in appropriated goods, and telephone and computer time is between $200,000 and $1.5 million.[263]

In Atlanta, a group raided the systems of about thirty companies and stole about $250,000 worth of hardware as well as uninsured company data stored on disks. Although the data loss was the greatest concern, the hackers weren't after the valuable data, but the inexpensive disks on which it was stored. Known as "The Assassins," this group was arrested and put out of business in early 1984. One technique they used was to take photographs, using a telephoto lens, through first-floor windows of computer codes and network passwords which had been carelessly posted on office walls.[264]

The "414s," named after their Milwaukee telephone area code, were another group of young hackers who, until the FBI raided them, broke into as many as sixty business and government computer systems in the U.S. and Canada, including those of the Los Alamos National Laboratory, Security Pacific National Bank in Los Angeles, and the Memorial Sloan-Kettering Cancer Center in New York. They changed some medical records at Sloan-Kettering, but backed off when they entered the bank's computer system. In the words of one of their members, then 17-year-old Neal Patrick, when they entered Security Pacific's system

> we knew it had something to do with world banking, because of instructions for a program to set various loan limits on countries around the world. All we did was look at the instructions because of what happened at Sloan-Kettering. We didn't want to take a chance on running a program on any countries.[265]

Another hacker, Lewis DePayne, received a five-month jail sentence for his hacking, which included data alteration. He was convicted of

---

[263] San Jose Mercury News, May 25, 1989.

[264] See note 38.

[265] Marbach, William D., "Beware: Hackers at Play," Newsweek, September 5, 1983, 42.

physically breaking into Pacific Telephone Co.'s San Francisco office and stealing sensitive system documents such as password lists and technical manuals. This information was later used to penetrate the company's mainframe computer and alter some of its key files by changing billing data and entering fake stop orders. DePayne pleaded no contest to charges that he used a system belonging to U.S. Leasing International, Inc., without authorization.[266]

That the threat is still very real was shown by the convictions, under federal law, of two hackers, Kevin Mitnick and Herbert Zinn, Jr., discussed in chapter 3. If the past is any guide, the high level of publicity given to these and other recent incidents such as the "Internet Worm" of November 1988[267] may inspire "copy-cat" cases of computer system crime and abuse. For example, Jay BloomBecker believes that prior publicity played a role in inspiring Stanley Mark Rifkin in his theft against Security Pacific National Bank.[268] And an editorial in Computerworld magazine recently speculated that

> the Tylenol poisoning scare of 1983 spawned a rash of copycat crimes, and a series of teenage murder suicides last Christmas appeared to relate to media coverage of earlier incidents. The specter of attacks striking computers worldwide should concern everyone who operates large systems.[269]

Even movies appear to influence hackers. According to Bill Landreth, the movie WarGames had a clear effect on his fellow hackers:

> Many, many people decided to try hacking on the basis of what they saw (or thought they saw) in

---

[266] Beeler, Jeffry, "Destroyed Files, Stole Documents: 'Phone Freak' Going to Jail for Two Schemes," Computerworld, June 28, 1982, 7.

[267] The alleged author, Robert T. Morris, Jr., was indicted in early August 1989, and subsequently convicted, under the federal Computer Fraud and Abuse Act.

[268] BloomBecker interview; Spectacular Computer Crimes, Dow Jones, Irwin, March 1990.

[269] "A Nasty Bug," Computerworld, April 4, 1988, 18.

> WarGames. Handles[270] like Warmonger, and esoteric references to Joshua (a key name in the movie) began to appear with distressing frequency.[271]

One may also speculate on the possible influence the September 26, 1988, Time cover story on "Computer Viruses" may have had on the author of the internet worm, which was released just over five weeks later.

Whether we consider hackers or thieves, the dollar losses to corporations from computer crime and abuse are large, although reliable estimates are hard to come by. Donn Parker of SRI, for example, has noted that unsubstantiated figures are often quoted and repeated.[272]

The accounting firm Ernst & Whinney estimated total high-tech thievery in the U.S. at between $3 billion and $5 billion annually, with average thefts of $500,000.[273] A 1986 survey of U.S. business conducted by Security magazine came up with average theft losses of $92,857, and that was skewed by one large million-dollar loss.[274] Preliminary data from a computer security census conducted by the National Center for Computer Crime Data and The Racal Corporation estimate the annual cost of computer abuse at $555.5 million, with average losses of $109,000. The census also indicates that computer crimes against banks are down from 18 percent of known crimes (in 1986) to 12 percent, but that commercial organizations sustain 36 percent of all computer crime, up from 23 percent in 1986.[275]

---

[270] Handles are assumed nicknames, such as "The Cracker," of hackers or communicators.

[271] See note 256 at 35.

[272] See "People, Not Systems, Key to Network Security," note 8; and Jack Dies Martin, "SRI Unit Leads Attack on Computer Criminals," The Business Journal - San Jose, February 8, 1988, 1.

[273] See note 78.

[274] Whitehurst, Susan A., "How Business Battles Computer Crime..." Security, October 1986, 56.

[275] "Crime Statistics," Communications of the ACM, June 1989, 657.

A final note about threats. Serious damage may be caused by simply the threat of a threat. That is, just as a traditional bomb scare can cause evacuation of a building with lost time and other expenses, the mere verbalized threat that a logic bomb is set to go off in a certain program may wreak havoc in a corporation. Policies and plans for the protection of information resources may need to address the possibility not only of a threat/actor causing actual damage, but also of being falsely threatened with a particular action.

4.2 SUSCEPTIBILITIES

The other side of the vulnerability coin from the chance events and hostile and non-hostile human agents is the openness of corporate information resources to damage, regardless of what caused it. It may be helpful to consider some of these susceptibilities – independently of who or what may exploit them – when developing corporate policies for the protection of information resources. Most of these concern actions or events involving the following:

- Alteration: Can programs or information be modified?
- Damage: Can the resource be physically or electronically impaired, so that it doesn't work properly?
- Deception: Can someone impersonate an employee, client, customer, or maintenance person? In person, or by using voice or data systems?
- Degradation: Can the information resource be slowed down in its processing or operation? Can the quality of operation be reduced?
- Destruction: Can the information resource be physically or electronically rendered inoperable?
- Disclosure: Can sensitive information be disclosed to unauthorized parties?
- Discredit: Can the integrity or reliability of the information resource be reduced in the eyes of various stakeholders?
- Disruption: Can the operation of the information resource be interrupted or otherwise manipulated?

- Duplication: Can information, data, or software be reproduced? How would this be detected?

- Interception: Can communications signals or other messages be intercepted by unauthorized parties? Would this be detected?

- Intrusion: Can an unauthorized person access the information resource?

- Termination: Can a communication or other information process be shut down?

- Theft: Can the information resource be stolen, or be used to steal from the company?

In thinking about a particular information resource's susceptibility to these sorts of actions, many methods or mechanisms for their occurring will be obvious, such as data alteration by an electrical power surge, or damage caused by fire or water. The following are some of the less obvious techniques and mechanisms by which these susceptibilities may come into existence:

- Crosstalk and electromagnetic interference (EMI) from one electronic system to another.

- Electromagnetic "leakage" of signals and information: "All electronic equipments emanate electromagnetic signals. Emanations produced by computers, terminals, and communication lines can be detected and translated into readable form by monitoring devices."[276]

- Loss of information in hard-copy formats, for example, by way of the trash bin or dumpster. "Hard-copy" here would refer to not only papers, documents, and computer print-outs, but also typewriter and computer ribbons, carbon paper, materials for graphics preparation, and so on.

It should be noted that in May 1988, the U.S. Supreme Court ruled, in a 6-2 decision, California v. Greenwood,[277] that Americans do not have a reasonable expectation of privacy concerning their garbage once it is off-premises. According to Robert P. Campbell, president of Advanced

---

[276] PC Security Considerations (Washington, D.C.: National Computer Security Center, December 1985), 4.

[277] U.S. 108 S.Ct. 1625 (1988).

Information Management, Inc., this means that "anything put into the trash becomes fair game."[278] Campbell suggested that snoops called "dumpster divers" are known to search for competitive intelligence, personal information on employees, system documentation and charts, logic designs, and passwords, among other items.[279]

In addition to some of the computer hacker techniques discussed above, a wide variety of techniques that may be used to intercept, intrude, and steal are technology-specific to computers and computer systems. A few of these techniques are described below.

Data Diddling. One of the most common methods, data diddling involves false data entries, or modifying data before or during its input to computers.

Salami Scams. In salami scams, a tiny amount of money may be skimmed in the hope that no one will notice or report the loss. For example, a penny is added to billing notices, the extra amounts are stolen, and the billing records are corrected. Even small amounts such as millage (the third decimal in rounding off interest payments) can amount to large sums in certain financial institutions.

Aggregation Attacks. For this method, individual pieces of information may be entirely worthless; yet, when pieced and matched with other pieces of information, they may reveal highly sensitive corporate or personal data. The fact, for example, that company organizational element XYZ is in R&D may be completely innocent. The fact that XYZ is studying a certain manufacturing process might also be worthless information, say, to a competitor. So might the fact that XYZ has some kind of deadline, and that XYZ is doing work associated with a particular contract bid. However, when all these facts are susceptible

---

[278] Betts, Mitch, " 'Dumpster Divers' Have Access to Data," Computerworld, May 23, 1988.

[279] Ibid.

to aggregation, a key piece of sensitive proprietary information may be revealed.

Trap Door. A very important hacker tool, the trap door is a hidden software or hardware mechanism (usually software) that permits normal system protection methods to be bypassed. Trap doors are frequently inserted in legitimate programs during their development. A programmer may simply want to make his development and testing job easier, or he may want to retain the ability to enter the system in the future. He may have intended to "close" the trap door after development, but forgot to do so. Once inside a system, a hacker will create one or more trap doors so that he can re-enter the system at will. The trap door may be something simple, such as creating new accounts, or it may be a sophisticated programming change to a mainframe's operating system. Bill "The Cracker" Landreth thinks trap doors are pervasive: "I've spent many hours in conversation with system operators and system programmers, and I would venture to guess that every large computer system in the world has some type of trapdoor built into it. Even video games and personal-computer software have trapdoors built into them. Trapdoors are just the kind of temptation that a programmer is utterly incapable of resisting."[280]

Super-user Status. A hacker's central goal is to obtain "super-user" status on a system, with consequent power over the operation of a system enjoyed by the legitimate system operator, or "sysop." Hackers can obtain super-user status in several ways:

1) Obtaining account information by calling and asking for it, impersonating employees, consultants, or maintenance personnel if need be

2) Obtaining access codes from other hackers, off of electronic bulletin boards, and so on

3) Wandering into a facility and obtaining such information, which may be posted near a terminal or otherwise written down

---

[280] See note 256 at 93.

4) Getting a few minutes to use a legitimate terminal, which may have been left on while not in use

5) Working from company telephone lists, which may contain data modem numbers

6) Searching through trash bins

7) Finding and using maintenance or test accounts, which may be used infrequently

8) Asking for HELP once online with a system

9) Guessing passwords for an account, which good hackers have turned into a fine art. Frequently, systems can be entered by trying insecure passwords such as "secret," "sexy," "password," "computer," "test," or even "God," a favorite of some system operators. "CEO" or "CFO" might even work. Files containing common first or last names can also be systematically and automatically tried, as many people select as passwords names of their spouse or family members. The same holds for ordinary words, as spell-checking dictionary files might be readily available on a target system. The so-called "hacker's anthem," by a hacker known as the "Cheshire Catalyst," illustrates this hack-hack technique:

> Put another password in, Bomb it out, then try again. Try to get past logging in, We're hacking, hacking, hacking.
>
> Try his first wife's maiden name, This is more than just a game. It's real fun, but just the same, It's hacking, hacking, hacking.[281]

Reverse Hack. Another twist is what Landreth calls the "reverse hack," in which a small set of common passwords is simply tried on many different accounts.

Special Keystrokes/Characters. A hacker may try to bypass a log-on sequence entirely by automatically sending a system rapid-fire sequences of keystrokes, or special control characters, such as CTRL-Z, to induce a system to default or go into an error condition. Having authorization for one level of command, he may insert a new command for which he isn't

---

[281] See note 265. Hackers' prowess generally does not extend to poetry.

authorized into a command buffer while the computer is verifying an OK for the lower-level command.

Decoy Program. A hacker might obtain a password using a decoy program, pretending he is the main system to an unsuspecting authorized user. The ability to manipulate the telephone system to re-route calls could be especially useful in executing a decoy. The authorized caller would see what appears to be a normal log-on sequence, and then send his password. Having obtained a valid password, the decoy would signal some sort of log-on failure and tell the user to hang up and call again. This time the call would be routed to the real system, and the user would never be the wiser.

Macro Commands. Many users of software communications programs have their passwords and log-on sequences stored in macro commands, which automatically log a user in with a minimum of keystrokes. Often these programs – with their macros – will be stored on hard disks, or on floppy disks which may be copied, loaned to someone, or thrown out in the trash.

There is an almost endless variety of such technical tricks available to would-be hackers and criminals. As computer hardware has more available memory, and as programs become increasingly massive and complex, it generally becomes easier to hide, and harder to find, trap doors, viruses, trojan horses, and so on.

Landreth notes that certain types of systems are especially attractive for, and susceptible to, hacker attacks. Among them are

1) Systems with many users. Sysops on such systems are usually very busy, and hackers can find safety in numbers. Also, more users means more passwords, and a greater opportunity to bilk an unsuspecting or careless user out of his account information.

2) Well-known companies. A hacker can enhance his reputation if he has the keys to the ABC corporation.

3) Service computers. Systems providing services such as information databases and games make the system a more attractive target.

4) Hacker-friendly systems. Some sysops allow hackers limited privileges, or otherwise tolerate trespassers.

5) "Easy" systems. These systems are known to contain exploitable weaknesses.[282]

And if all else fails, there's always an insider who might be willing, induced, or fooled into assisting an unauthorized person to get into a system. Noel Matchett emphasizes that one point is continually brought up by his clients: "Our weak point is our people."[283]

When corporations were asked by the 1986 Security magazine survey about their three biggest threats to computers and data in their companies, they responded as follows:

70% - Unauthorized use by employees

49% - Routine errors and omissions

38% - Carelessness with printouts

36% - Theft of computers

25% - Fire damage

24% - Use or misuse by outsiders

19% - Vandalism, floods, or other disasters[284]

We have surveyed the most important types of threats to, and susceptibilities of, corporate information resources. By considering the value of an information resource, together with the kinds of threats and susceptibilities which, when combined suggest its vulnerability, management may be able to come to a reasonably informed assessment of the need to protect the resource. After those information resources

---

[282] See note 256 at 108-10.

[283] Noel Matchett interview.

[284] See note 274 at 58.

which are more valuable (and more vulnerable) than others have been identified, a foundation will have been built upon which management can select the levels and types of protection most appropriate for its particular circumstances.

CHAPTER FIVE

PROTECTION

Corporate policies for the protection of information resources can be built upon a variety of options, which fall into several categories. These measures are grouped according to the nature of the type of protection, rather than by the threat or susceptibility which they are designed to reduce. The major categories are

1) Information resource (its reduction or elimination)

2) Education

3) Contract services (use of, such as disaster recovery)

4) Aggressive legal action

5) Published company procedures, codes, and policies

6) Technical measures

7) Insurance

On one level, the goal of such measures is to ensure the integrity, confidentiality, and availability of information resources. On another level, the aim of corporate policies is to <u>prevent</u> damage, <u>detect</u> damage and its cause, <u>limit</u> any damage, and <u>recover</u> from any damage in a cost-effective and timely manner.

While reviewing the checklist of options, keep in mind these few basic principles and ideas:

- It is unlikely that any single approach to protection will provide adequate protection. A mix may be not only more effective, but also less expensive.

- The majority of protection options have important dollar and operational tradeoffs. As a general rule, the better the protection, the more it will cost in dollars and operational overhead and hassle.

- Over-reliance on any one approach can easily result in a false sense of security, which may produce worse results than if everyone recognized that there was little or no security.

- Some options are inexpensive or relatively painless to implement, making them attractive.
- Every protection method has pitfalls and "holes." Perfect security is not feasible.
- "Every business in business is at risk: either you accept it, avoid it, transfer it, or control it."[285]
- As elsewhere, common sense may be the most important element. It is easy to focus on the details of a particular approach, and thereby lose sight of the overall goal.

The remainder of this chapter describes the seven approaches to protection listed above.

5.1 THE INFORMATION RESOURCE

This frequently overlooked option may prove useful in certain circumstances. For example, it may be the case that if a particular information resource exists, its value (in terms of legal considerations) and its vulnerability may indicate that it needs to be protected by one means or another. But it may also be the case that the information resource itself may not be needed by the company; or, it could be reduced in size (number of terminals, and so on) or some other manner that could affect the protection options available for it. The question, Do we even need to <u>have</u> this information resource? is offered for consideration as a first step in determining which protection approaches, if any, to use.

5.2 EDUCATION

Virtually every expert, professional, technician, hacker, criminal, or security specialist – nearly everyone – who has thought about or studied the issue of protection for information resources has come to

---

[285] Marr Haack, director, Marketing, Electronics & Information Technology, St. Paul Fire & Marine Insurance Co., interview with author, May 22, 1989.

the same conclusion: educating users is the single most important, and single most neglected, security measure that can be taken.

If Bill Landreth had a primary theme and message in his book about computer hackers, it was that companies should educate, and educate, and then educate system users some more. According to Landreth, "If they did, hacking as it is today would fall to such a low level of activity it could be considered dead."[286]

Education – about how information resources work, how valuable and how vulnerable they are, about how to protect them, and about who is responsible for what – is in and of itself a highly cost-effective protection measure. More than that, however, it is an often necessary step in the effective operation of other types of protective measures.

One mistake some companies make is that they view education on the protection of information resources as something that should be limited to the "techies" in the computer room. The following example illustrates what this view can lead to. A Fortune 500 company recently installed an executive information system for its top managers, but no one taught the executives about network security. One vice-president was so pleased with the system that he described it in a lecture, which was attended by some of his competitors. In his description, he read aloud the special telephone access number for the network, which resulted in several people from the audience trying to access the system.[287] The company claimed that no information was damaged or stolen, yet the unauthorized callers were a five-letter password[288] away from having access to the company's most sensitive information.[289]

---

[286] See note 256 at 126.

[287] Crockett, Barton, "Securing Corporate Networks," Network World, March 21, 1988, 17.

[288] This password was perhaps his wife's name.

[289] See note 287.

A somewhat cynical view of management's knowledge of information resources' value, vulnerability, and protection was related to Jay BloomBecker at a computer virus conference:

> A computer security professional said: "The guys upstairs are real jerks [to be charitable]. They don't know anything about security, they know very little about computers, and that's more than they want to know. All they know is what's in Time magazine. If I want to get money for something, and they've read about viruses, whatever the problem is, I'll call it a virus problem. Do I need uninterrupted power supplies? I'll say, you know, without it we have viruses. . . . Do I need training in database management? Without it we're going to have viruses!"[290]

These stories suggest that education probably could be more effective if it were not confined to information resource technicians. For protection policies to work, all levels of employees who have anything to do with information resources need to be reasonably well-educated about security. This even includes after-hours cleaning personnel, who may represent a particularly weak link in the chain. Charles Zraket, CEO of the MITRE Corporation, sums it up well:

> In the last analysis I've always felt, as a CEO, that the management has to have control over its information resources. . . . and I include here understanding what the system is, and how it works, and what it's capable of, and what it is you want to protect, and why.[291]

Some factors to consider in implementing education as a way to protect information resources are listed below:

- Tailoring education to different levels, but including everyone who uses or has potential access to information resources
- Incorporating such training into indoctrination and familiarization for new employees

---

[290] BloomBecker interview.

[291] Charles Zraket interview.

- Addressing what the information resources are, where they are, who's responsible for them, why they are valuable, how they are vulnerable, and how employees are expected to protect them
- Addressing whom to go to with questions, for advice, and to report suspected problems
- Addressing all company policies that relate to security
- Ensuring periodic follow-up education
- Using existing corporate internal communications, such as hall posters, electronic mail, and bulletin boards for continuing reminders

5.3 CONTRACT SERVICES

Contract services and consultants that specialize in security for information resources may be useful in developing and implementing corporate policies. Because they are not part of the company, they may be especially useful in identifying vulnerabilities and protection options which have been overlooked.

Perhaps the most useful contract security services are those offering off-site communications, data processing, and data backup services. Specializing in the area known as "disaster recovery," such firms, although expensive, may be cost-effective. One of the companies hit hard by the Hinsdale fire, for example, was United Stationers. Since 1982, it had spent almost $1 million per year to have a disaster recovery service back up its Forest Park computer facility. With a prepared disaster recovery plan, the company was able to resume full operation within one day using alternate processing and communications facilities. According to CEO Joel Spungin, United Stationers saved at least $30 million in sales during the time Hinsdale was out and, perhaps more importantly, boosted customer confidence.[292]

Disaster recovery firms offer a wide variety of services, ranging from assistance with disaster recovery (or what Donn Parker has called

---

[292] See note 32, Wall.

"business continuity" planning) to the provision of "hot sites" equipped with the necessary hardware, software, and data to immediately take over for a facility which has experienced a disaster. Some elements of an adequate disaster recovery plan are that it

- Address the operations of at least three different levels: end users, ADP and communications centers, and the organization as a whole.
- Be prepared with participation of all relevant corporate organizations, such as security, sales, operations, procurement, collections, R&D, technical support, accounting, payroll, facilities or building management.
- Specifically address data backup, software backup, alternate data processing capabilities, backup staffing, backup supplies, and emergency response procedures (who activates it, how is it activated, how is it terminated, communications, and so on).
- Allows for, and is, in fact, periodically tested under no-notice conditions.

Jim Domanico has identified four common mistakes in recovery planning:

1) Not assigning more than one person to do all the planning
2) Not documenting the plan
3) Not updating the plan
4) Not testing the plan[293]

In a similar vein, Philip Rothstein has proposed a list of questions that top management might ask to ensure that the plan will work. Among them are the following:

- Is the disaster recovery function adequately staffed and funded?
- Is disaster recovery a consideration integral to all planning throughout the organization?
- Are there adequate – and impartial – reviews?

---

[293] Domanico, Jim, "Users Plan for the Worst," Telephony, October 17, 1988, 56.

- Is the plan continually maintained, updated, and tested?
- Is the plan concise? Understandable?
- Is the plan's activation and deactivation process and responsibility clearly defined?
- Does the plan follow through to recovery? How far does it go?
- Are human elements addressed? Can people be expected to perform their assigned roles under stress?[294]

But disaster recovery and business continuity involve more than simply preparing a plan and contracting for backup service. The following checklist of items might assist in a smooth recovery:

- Periodically review the security of off-site storage.
- Ask common carriers and other significant service providers about <u>their</u> contingency or recovery plans. What alternate capabilities exist (for example, mobile communications vans)?
- Make sure that clear procedures are available to power-down any system or building in an emergency.
- Consider manning critical facilities 24-hours a day.
- Implement procedures to make sure that key personnel are available, and can be located and contacted.
- Review Federal Information Processing Standard (FIPS) Publication 87 – "Guidelines for ADP Contingency Planning."
- Store data and software backups off-site.
- Store a copy (or copies) of the disaster recovery plan off-site, and where they are readily available in an emergency.
- Ensure that enough key employees have the necessary information to activate emergency plans.
- Make sure that clear, comprehensive documentation is available that describes how to operate critical systems.

---

[294] See note 211 at 86–98.

- Try to incorporate route diversity and redundant network architectures into critical systems.[295]

- At reasonable intervals, make up hard-copy, non-magnetic backups of critical data and custom software.

- Make sure that recovery backups are made frequently enough so that the data are useable, so that backup information is adequately up-to-date.

- Consider using disk-less terminals to make sure that backups are made (also providing anti-virus/worm protection, and protection against copying or loss of data and programs).[296]

- Make sure that alternate power sources for electronic access control systems are used.

Additional items for consideration that may affect business continuity and disaster recovery are included in the miscellaneous checklist below.

One yardstick to consider in determining how much to spend on disaster recovery, if anything, has been provided by Richard Reese, president of Iron Mountain, a records-management firm. Reese maintains that

> affordability depends on how much of a premium companies are willing to spend. Typically, 1 to 3 percent of your DP budget is spent on [records management and recovery]. For smaller companies it is 3 percent or more.[297]

---

[295] John F. McLaughlin advises caution so that redundancy is not illusory. "A corporate user who loses service on its AT&T circuits does not achieve much redundancy if its second carrier is a reseller dependent upon the same AT&T facilities. Absolute physical separation of plant is required to achieve real redundancy." From: McLaughlin, John F., "Using Competing Carriers to Ensure the Survivability of Corporate Information Systems" (Cambridge, Mass.: Program on Information Resources Policy, Harvard University, November 1987), 2.

[296] End-terminal users of PC-based systems often fail to back up their data. Disk-less systems allow for the central data processing element to back up all data since it's stored in a central location, not on local terminals. Anti-viral and related protection is provided since disk-less terminals do not allow local users to run (possibly infected) software.

[297] Corliss, Ellen T., "Prepare for the Worst," Massachusetts High Tech 7, no. 2 (November 7-28, 1988).

5.4 LEGAL ACTION

Yet another approach to protecting corporate information resources is to adopt, and pursue, an aggressive legal posture. The basic goal would be to increase deterrence of crime and abuse of information resources by pressing criminal and civil cases through the legal system in a highly visible manner. This approach can be costly – especially in the short run – but for companies with large dollar amounts at stake, it might pay security dividends to be known as a "tough" company to steal from, hack into, or otherwise fool around with. And the threat of a hard-line legal response probably does have merit as a deterrent. Bill Landreth believes that, as a rule, hackers "would like to stay out of legal trouble, if possible."[298]

As noted in the legal considerations section of Part Three, much of the law dealing with information resources is relatively new, waiting to be tested in court. The effectiveness of a hard-line approach remains to be demonstrated. In other areas, however, a change in corporate attitude and policy towards fighting it out in court may have changed outside behavior towards the company.

For example, among the recent financial troubles reported about the Piper Aircraft Company, not the least were the 60 potentially crippling product-liability suits alleging poor design and manufacturing. The first steps of M. Stuart Millar, a new CEO, were to cancel Piper's expensive insurance policy, set up a reserve fund for potential damages, and "hire lawyers to fight to the finish any suit he deemed unwarranted."[299] As a result, the company's estimated 1989 legal fees are currently less than the cost of the former insurance, and "far fewer lawsuits are being filed."[300] Although it is difficult to tell whether fewer lawsuits are being filed because Piper no longer carries

---

[298] See note 256 at 60.

[299] DeGeorge, Gail, "Piper May Still Be Carrying Excess Baggage," Business Week, June 12, 1989, 76.

[300] Ibid.

insurance, or because of the get-tough policy, it appears that the hard-line policy has had at least some deterrent effect.

5.5 COMPANY PROCEDURES, CODES, AND POLICIES

A relatively inexpensive approach to the protection of information resources is to issue carefully crafted corporate policies, procedures, and codes of behavior. In addition to codes of ethical behavior, discussed in chapter 3, corporate policies and procedures might establish, require, or address the following procedures:

- Establishing an information resources security committee
- Having employees sign security statements, non-compete agreements, and so on
- Requiring employees to take earned leave[301]
- Screening outside auxiliary personnel (for example, the cleaning force)
- Establishing a "waste, fraud and abuse" hotline, with rewards for valid reports
- Periodically reassigning key information resource personnel
- Establishing an after-hours "clean-desk" policy
- Prohibiting "piggy-back" or "tailgating" access[302]
- Requiring users to electrostatically ground themselves before handling disks, PCs, and so on
- Identifying information resource auditing and maintenance personnel, and the way that they will be identified
- Requiring at least two people to be trained in the operation and maintenance of any critical systems

---

[301] Problems caused by an employee who has "gone bad" may be more likely to show up when that employee is not around to cover up any wrongdoing.

[302] The common situation which occurs when a person with authorized access enters a space, and a second person follows the first into the space, without having to use a key, cipher lock, or other access control device.

- Implementing an information classification policy, with marking procedures, such as "privileged," "confidential," and "company use only"
- Making security awareness and conduct a part of performance appraisals
- Publishing or announcing disciplinary actions for failure to protect information resources
- Establishing procedures to screen prospective/new employees
- Establishing procedures for an employee assistance program (EAP)
- Establishing policies and procedures restricting the use of freeware, shareware, and other personal software on corporate computers
- Requiring security assessments as part of all major purchases and contracts
- Requiring written approval to remove hardware, software, or data disks
- Implementing a standard disk marking system and inventory control system
- Establishing a periodic (for example, annual) data housecleaning day
- Spreading critical approval authority between two or more people (for example, separate input, authorization, and review functions), and establishing clear spending levels of authority
- Prohibiting same-person access to both primary and backup critical data, software, or hardware
- Establishing no-lone-zones, that is, sensitive physical areas where two authorized employees always must be present
- Establishing a hierarchy of physical security zones
- Requiring the routine, periodic destruction of out-of-date and unneeded data
- Establishing controls on photocopiers (for example, access and use of special papers that are difficult to copy)
- Prohibiting the use of company computers for personal business
- Prohibiting the copying of licensed software, or the use of bootlegged copies

- Keeping and updating an inventory of equipment, software, and other information resources

- Limiting PC use to a single person, so that accountability can be maintained

- Changing locks, keys, codes, and passwords after

    1) A security violation

    2) Someone with access leaves (for any reason)

    3) A designated period of time (for example, 3 months)

- Requiring equipment (especially modems) to be unplugged and disconnected during overnight/weekend periods, office open-house periods, thunderstorms, and so on

- Requiring all media, and all equipment, to be labeled with an indication of the highest level of sensitivity of information which may be processed on that machine

- Controlling the destruction of used media

- Spelling out procedures for removing retiring, departing, and terminated employees from access to information resources

- Implementing formal controls for the selection, purchase, acceptance, testing, and modification of information resource software and hardware

- Encouraging strangers to be challenged, or building security to be called when strangers are discovered

- Requiring that decisions on protecting information resources (or not protecting them) be properly documented

- Establishing periodic inventories and assessments of information resources

- Ensuring that auditing staffs address information resources and their protection

- Ensuring that tests and audits of information resources are a surprise

- Requiring backups of data frequently enough to ensure up-to-date, useable information

- Establishing a "black hat" team to actively test the protection of information resources

- Establishing clear procedures for identifying key operational, security, and maintenance personnel, so that impersonation would be difficult
- Implementing controls on all trash and garbage
- Avoiding reliance on security vendors for security advice

Many procedures in the checklist above can be implemented in reasonably short time periods and at modest cost. Two qualities of special value in preparing such policies – as with all policies – are brevity and clarity. The company with the worst code of ethics or emergency procedures is the one with four volumes devoted to each purpose.

5.6 TECHNICAL MEASURES

Even with judicious use of insurance, education, legal action, policies and codes, and contract services, most corporate policies for the protection of information resources will probably include the use of various technical measures to prevent, detect, and limit damage, as well as assist in recovering from accidents, disasters, and attacks.

Because such a wide array of technical devices and techniques is available for use today and is growing rapidly, it would be impossible to list them all. What may be helpful, however, is a checklist of techniques, hardware, and software which, in one way or another, provides a measure of protection against the various threats and susceptibilities discussed earlier in this report. These are listed here for consideration of their utility for particular information resources at particular corporations. Many of them may represent overkill; others clearly may be necessary and worth the effort. The checklist starts with measures that are miscellaneous or general in nature, and ends with those that are targeted more precisely at computer hackers and criminals. They are loosely grouped as follows:

5.6.1 General Purpose, Physical Security Measures

- Use document shredders, magnetic degaussers, and destruction equipment
- Contract with a document disposal service
- Destroy or otherwise control printer/typewriter ribbons and carbon papers
- Store disks in locking cabinets and data safes that are waterproof and fire-resistant
- Install security glass or glazing in appropriate locations
- Install access controls such as

  1) Cipher locks/keypad entry systems
  2) Mechanical locks
  3) Magnetic card systems
  4) Smart card systems
  5) Biometric systems that measure finger or palm prints, voice prints, or retinal blood vessel scans
  6) ID card systems
  7) Door alarms
  8) Visitor logs and escort system
  9) Video surveillance
  10) Guard dogs and other "bio-sensors"

- Implement regular risk assessment programs, including use of software-assisted programs
- Install intrusion detection systems and alarms, such as perimeter alarms, ultrasound or infrared motion detectors, and alarms that directly alert the police or security force
- Install fences and adequate lighting
- Establish and support a professional guard force
- Mark hardware and software with the company's name, and register it with police identification systems
- Test intrusion detection equipment and procedures

- Install automatic locks on doors to all rooms containing information resource terminals or critical information
- Use anchoring/locking devices for PCs, small equipment, software, and data
- Locate video displays/CRTs away from windows, doorways, and passageways
- Lock and protect backup disks against water or fire damage with the same care as primary disks; as a general rule, backup disks should be controlled in the same manner as primary disks
- Keep equipment clean by using dust covers (preferably waterproof plastic) and limiting food and beverages as well as smoking near information resources
- Prevent trash buildup and dust accumulation
- Handle all magnetic media carefully, using dust jackets, for example
- Ensure that air conditioning and heater vents stay open and clear
- Filter air to remove contaminants
- Lease or buy earthquake-resistant building structures
- Shock-mount sensitive information resources in areas where earth tremors are likely
- Install window shutters to protect against glass breakage in storms or during earth tremors
- Screen windows and air vents to protect against volcanic ash and other airborne contaminants
- Place hardware and software only on sturdy furniture
- Use special computer disc mailers when mailing magnetic disks

5.6.2 Water/Moisture Protective Measures

- Don't locate hardware or equipment under water pipes or where direct sunlight may shine on it
- Re-route water pipes
- Install moisture detectors
- Seal passageways for water (for example, install dams, moats, or pumps to control water leakage)

- Install water detectors, such as area or tape (water-sensitive) detectors
- Clearly mark emergency water shut-off valves
- Regularly test water and moisture detectors
- Use waterproof containers for critical data or software

5.6.3 Fire Protection Measures

- Install fire alarms that directly alert fire departments or security response teams
- Give local fire departments blueprints or other information which may be of use to them during an emergency; work with them <u>before</u> an emergency occurs
- Remove flammables from critical information resource areas
- Locate printers, copiers, coffee-makers, and other fire-potential equipment in containment zones
- Install adequate smoke and fire detectors
- Install adequate fire suppression equipment, such as sprinklers, gas fire supression devices, and other extinguishers
- Test fire detection equipment and hold no-notice fire drills (testing of all emergency equipment and procedures cannot be overemphasized, and is often ignored)

5.6.4 Electrical/Power Protective Measures

- Use power surge protectors
- Install lightning arrestors
- Remove coffee and popcorn makers, hot plates, refrigerators, and so on, which may cause voltage fluctuations
- Install power supplies that cannot be interrupted
- Use anti-static sprays, pads, carpets, and cleaners; provide a convenient electrostatic ground near all computer, switching, and other static-sensitive equipment or media

5.6.5 Communications Security Measures

- Contract for protected services by common carriers to increase telephone security
- Use encryption equipment
- Purchase and use secure telephones

5.6.6 PC/Network Protective Measures

- Power down computer terminals between different users, or levels of sensitivity of use, to prevent unintended access to files or data
- Back up data frequently, especially on PCs. For critical data use multiple discs, and multiple filenames that are not similar, to prevent accidental erasure
- Identify and reduce the number of critical hardware, software or data single-failure points, that is, points of non-redundancy in the information resource
- Don't trust the IBM/MS DOS and similar operating system ERASE commands to eliminate data. They only block out the filename and zero the disk's File Allocation Table; the data is still there until it is written over
- Overwrite sensitive data on hard and floppy disks with all 1s, then all 0s, and then random 1s and 0s
- Be especially careful about entering sensitive information onto hard disks, because it's difficult to remove without degaussing the entire disk
- Purchase and use only high-quality, brand-name media
- Degauss hard disk drives before sending them out or allowing maintenance work on them
- Consider purchasing equipment with anti-tamper features
- Have the computer system or log-on system shut down for 5 to 15 minutes after a preset total of incorrect log-on attempts
- Have the system transmit a security notice before hanging up
- Have the system notify all users, when they first log on, of their previous log-on time and date, and require them to verify the information
- Restrict the system from giving out any information before a correct log-on procedure has been executed

- Use call-back units, but have them call out on a different line from the incoming call

- Use filter systems (requiring an ID, PIN, or other code before the call is passed on to the information resource)

- Employ security programs that identify remote users by their unique keyboard/keystroke use

- Employ audit trails and auditing software that analyze account activity and notify the sysop of anomalies

- Have the phone company reclassify data grade modem lines to voice grade, so they will not stand out in phone company records as modem lines

- Periodically change modem telephone numbers

- Have modem numbers listed with 3-digit exchanges that are different from regular company voice lines; make sure the modem number is not published or given out to non-users

- Periodically and routinely remove/erase old and unused accounts

- Have an operator or recorded voice answer the phone, to get a request for connection to a data port

- Program the system computer/modem to wait several rings before answering

- Ensure that the system logs off callers who hang up or who are disconnected before they log off

- Shut off and lock terminals if users are going to be away for a period of time

- Buy and use removable (lockable) hard disk drives

- Split critical computer system knowledge so that no one person has total access or control

- Employ message authentication equipment and schemes to verify that a message is from its purported source

- Use checksums, and especially cryptographic checksums, to verify that a file or program has not been modified; they offer strong protection against an undetected virus, trojan horse, and so on

- Establish strong password management controls

- Never share passwords

- Immediately change initial default passwords (just like factory pre-set safe combinations must be changed for security), and periodically thereafter

- Have individuals personally pick up and sign for passwords

- Use layered password systems, that is, different passwords for different levels of access and privilege

- Use passwords or passphrases that are

    1) As long and random as can be remembered (rather than written down) by users, such as compound passwords (for example, DANIEL.VERB), or compound passwords based on the first letters of an unusual phrase (for example, "the boss really loves me") coupled with a compound (for example, TBRLE.BB for "Billy Bob")

    2) Computer-generated

- Encrypt and carefully control access to password files

- Limit or eliminate type-ahead character-storage memory buffers on networked systems (to avoid hack-hack and rapid keystroke attacks)

- Allow a caller only one, two, or three log-on attempts before hanging up

- Use only write-protected or notchless floppy disks to boot up a PC

- Use the system to put out frequent security tips and educational items

- Reduce the number of terminals

- Limit incoming/outgoing calls to specific exchanges or area codes

- Allow only remote callers to transmit, but not receive, data (if the nature of the system permits it)

- Review any outside or suspicious software on a completely isolated system before allowing use on company systems

- Purchase and use answer-back systems for remote terminals (unique terminal IDs are automatically transmitted to the network host)

- Use encryption with dial-back and filter systems

- Never boot a hard disc system from an unknown floppy (to prevent picking up a virus, worm, trojan horse, logic bomb, and so on)

- Buy and use virus detection, "vaccination," and eradication software

- Encrypt stored programs and data files

- Put appropriate information into read-only files

- Set and monitor system usage limits by individual accounts

- Purchase and install high-quality mainframe security systems (which allow programming of many suggestions in this checklist)

- Consider dedicating selected PCs to online activity, keeping them separate from offline use

- Use software to check for input errors, for example

    1) Character checks (numeric or alpha)

    2) Range checks (data within preset limits)

    3) Relationship checks (against a master file or record)

- Purchase and use pre-formatted disks (to reduce likelihood of accidental FORMAT commands wiping out data)

- Keep magnetic fields, such as telephone handsets, away from magnetic media

- Clean disk drives regularly

- Pack and lock hard disk read/write heads before moving the system

- Use "smart cards" or "super smart cards," which contain electrically erasable programmable read-only memory (EE-PROM) for interactive authentication of remote terminal users

- Ensure that audit procedures are embedded into a computer system's design

- Ensure that employees know that there is an audit system, but do not reveal all the details to them

- Use non-standard devices or protocols (to reduce hacker access)

- Control or restrict the use of automatic log-on macros in communications software programs

- Remove passwords and other account information from communications software disks before they are destroyed, removed, or loaned

- Be alert for hacker tracks:

  1) Overused accounts

  2) Accounts used by absent people

  3) Unusual times of computer activity

  4) Excessive use of HELP files

  5) Unusual use of files

- If a hacker is encountered on a system, treat him carefully. Don't bluff, or be abusive. Bill Landreth recommends these five steps: identify, confront, try to enlist his help, neutralize, remove.[303]

5.7 INSURANCE

Having reviewed its options for reducing information resources, educating system users, obtaining disaster recovery and other contractual security services, pursuing aggressive legal action, publishing company policies and procedures, and employing technical measures to protect information resources, corporations may still find gaps where their policies do not match the security requirements of the assessed value and vulnerability of their information resources. At this point, corporations may consider negotiation for appropriate insurance coverage.

Insurance is sometimes overlooked as a useful tool for managing the risk to information resources – versus other resources – for reasons touched on earlier, such as the "softness" which exists in the perception, definition, and value of information resources regarding other more tangible assets. For example, insurance protection for a fleet of delivery vehicles has a variety of clearcut factors at work.

---

[303] See note 256 at 195-206. See this section for a more detailed set of suggestions on how to handle a hacker, once detected.

One such factor is the clear perception of the assets' value and its vulnerability to damage. This results in an easy acceptance of the need for insurance, and little confusion over how much the owner is willing to spend. Among other factors are clear analogs with the individual manager's personal experiences in insuring his private vehicles (or house, life, health, and so on). That personal-experience analogy is usually lacking when the subject is information resources.

A second important factor is that of outside requirements, such as those mandated by law (for vehicles), or by financial backers for other sorts of real assets. Richard S. Banas, vice-president (Electronics Industry) for St. Paul Fire & Marine Insurance Company, emphasizes the role of financing in requiring insurance:

> When you buy a $100 million building, or a $5 million piece of equipment, that lender is requiring insurance coverage. When you're talking about information flow and revenue generation, or even business interruption, in traditional kinds of industries, no lender is sitting there saying "give me the policy before I give you the loan," and the stockholders maybe should do that . . . saying give me a guarantee that you're going to continue to produce.[304]

Whether or not specifically required by law, lenders, and stockholders, insurance represents a potentially cost-effective approach to the protection of corporate information resources.

Available data seem to suggest that the insurance approach to protecting[305] information resources is gaining acceptance. At a minimum, the writing of policies to protect information assets has been growing steadily. The Inland Marine Underwriters Association, for example, reports that earned premiums on electronic data processing (EDP) policies have increased more than 400 percent from 1980 to

---

[304] Richard S. Banas, interview with author, May 22, 1989.

[305] Not in the sense, of course, of preventing loss, but "protecting" the corporate values associated with any loss.

1986.[306] Marr Haack of St. Paul Fire & Marine also notes that in the wake of the Hinsdale fire, his company has received more queries from businesses concerned about insuring their communications.[307] The Hinsdale fire, in particular, may have kindled interest in insurance since a track record had already been established in which fire is the main cause of insured losses to EDP equipment.[308]

Although the basic concepts behind insurance policies are familiar to all, the specific types of policies and coverage offered vary widely in time and space. That is, the policies offered are constantly changing over time. Also, since almost all insurance regulation is performed on a state by state basis, coverage available in California may not be available in Arizona or elsewhere.

The basic approaches to insurance coverage for information resources address compensation for

- Damage or theft of equipment and component parts, information media such as magnetic disks and tapes, and designated "valuable papers."
- Extra expenses incurred as a result of damage to an information resource (for example, cleaning up after a fire).
- Losses due to interruption of business.[309]

With respect to insuring against liability of corporate officers for failure to adequately protect information resources, there are two basic approaches. One is having adequate Directors and Officers (D&O) insurance, which is designed to protect against financial liability for failure to exercise "due care and diligence." Another approach (for

---

[306] Schiff, Samuel, "The Automation Policy," Insurance Review, January 1989, 37.

[307] Haack interview.

[308] See note 306.

[309] Bigelow, Robert P., "Data Processing Insurance," Computers & the Law: An Introductory Handbook, 3rd ed. 1981, American Bar Association, 232-33.

protecting key individuals) is to consider indemnity agreements between them and the corporation in which uninsured liability is indemnified (or transferred) to the corporation. As Randall Miller has cautioned, however, most such D&O policies and indemnity agreements do not cover failure to exercise the "duty of good faith." In particular, he notes:

> If you know there is a real and preventable risk to your corporation and you do nothing to prevent the risk, then your disregard for the proper course of conduct would probably be construed as acting in bad faith.[310]

Another basic type of insurance coverage potentially important to both business vendors and customers (of hardware, software, and services) is known as errors and omissions (E&O) insurance. E&O insurance is designed to cover consequential damage claims that may result from errors, omissions, and even negligent acts committed (or omitted) during the course of business. An example would include the case of a software provider whose errors in software design caused consequential damage to a user or other third party. As such, service providers and those companies which perform data processing and similar functions (including disaster recovery) may want to carefully consider this form of insurance protection.

Some other policies, coverages, or standard "floaters" which may be considered for the protection of information resources are listed below:

- Standard commercial property
- Blanket earnings and expenses
- Data processing property
- Manufacturers output
- Specialty coverage (on things such as prototypes and project R&D)
- Accounts receivable
- Employee dishonesty

---

[310] See note 109 at 74.

- Transit
- Salesman's samples
- Installation
- Maintenance
- Exhibitions

Of course, it may be possible to negotiate customized insurance policies for corporations that have a clear idea of the identification, value, and vulnerability of a particular information resource. Because it can be very difficult to identify and anticipate potential kinds of losses, however, and anticipate various technicalities hidden in contracts, as a general rule it may be advisable to obtain as general as possible coverage for broad classes of information resources. It is difficult to name all likely perils in "Named Peril" insurance, for instance.

To offer an analogy from life insurance, many insurance companies offer special policies or floaters to cover death caused by cancer. These may seem attractive if one believes oneself highly susceptible to the threat of that particular disease. Yet, it sometimes happens that someone develops cancer, enters a terminal stage, and then dies of other causes which may or may not be associated with cancer. For example, certain cancer treatments may leave patients exposed to pneumonia. When patients are in such a terminal stage, they and the medical providers may decide to let them die of pneumonia. In this case the cause of death will normally be listed as "pneumonia," and the cancer coverage may not apply.

This example is simply indicative of the potential pitfalls of specialized insurance. It may pay to ask if a general coverage includes a specific concern of the corporation. The recent advent of computer viruses, for example, has been addressed by one large insurer as part of its E&O policies for software manufacturers. Another major underwriter takes the approach that its E&O policies don't specifically exclude viruses, and yet another considers a virus as part of its coverage

against vandalism or malicious mischief.[311] When considering insurance as a protective measure, top management may want to keep in mind many other factors, such as the following.

Valuation Methods.

1) Actual cash value

2) Replacement costs

3) Functional replacement costs

4) Market value

5) Manufacturer's selling price

6) Valued amount (direct, or indirect)

Insurance. Corporations should consider insurance like E&O, which is carried by its vendors and suppliers of hardware, software, and services. Corporations may want to query prospective contractors as to the adequacy of their insurance. A case currently under appeal illustrates both the high stakes that can be involved, and the difficulties which might have been avoided by careful contracting, and attention to E&O or similar insurance up front. Geophysical Systems Corporation, an oil-surveying company, went into Chapter 11 bankruptcy, which it blamed on faulty hardware and software the company had purchased from Seismograph Service Corporation. A California court granted Geophysical $48.3 million in damages (although the company claims it lost business worth twice that amount). An article in The Economist warns that

> Seismograph Service, like most similar companies, is not insured against litigation from a customer. . . . Limited protection can be found but, since it is a new field, most insurers are too short of actuarial statistics to price general policies.[312]

---

[311] Chubb Group, St. Paul Fire & Marine, and Fireman's Fund, "As Computer Virus Fears Grow, Insurers Focus on the Coverage Question," Wall Street Journal, June 1, 1989, 1.

[312] "Computer liability: Suing for Bugs," The Economist, January 7, 1989, 61.

Time or Geographical Limits in Coverage.

Coverage Limits and Maximums.

Deductibles. Typical computer facility deductibles, for example, may include separate deductibles for mechanical breakdowns, fire and related perils, business interruption, and extra expenses.[313]

Requirements for Other Protection Steps. If such requirements are not taken or are allowed to lapse, a corporation's insurance coverage may be invalidated. According to computer lawyer Susan Nycum, the key to lowering liability exposure is being "prepared to show you've done everything to eliminate software errors."[314] And Marr Haack notes that for his insurance company, the protection steps taken – especially disaster recovery – affect the amount of insurance needed, and the premiums paid.[315] He asks: Why should insurers agree to assume information technology risks when many of the practical solutions available to minimize these risks have not been implemented?[316]

Exclusions for Other Concerns. Corporations should consider these exclusions as well:

1) Other insurance coverage

2) Bodily or personal injury

3) Intentional or dishonest acts

4) Violation of laws or regulations

5) Copyright or patent infringement

---

[313] See note 306.

[314] Joyce, Ed, "Software Bugs: A matter of Life and Liability," Datamation, May 15, 1987, 88.

[315] Haack interview.

[316] Haack, Marr T., "Practical Techniques for Management of Computer-Related Risks," paper presented at the Practical Computer Law Strategies Conference, March 2-3, 1989, sponsored by the Georgetown University Law Center, Washington, D.C.

6) Warranty coverages

7) Professional liability

8) Pollution and toxic wastes

9) Breach of security

The fire at Hinsdale underlines the importance of exclusions. Many companies that were insured under business-interruption policies found, to their dismay, that their losses were not covered because the coverage was excluded by losses caused by off-site events; only on-site damages by fire, flood, and so on were covered.[317]

Contract and Policy Negotiations. Robert Bigelow noted a basic rule of contract law: "He who writes the document is the one against whom any ambiguities are construed," yet "the doctrine doesn't apply if there's been a lot of negotiation."[318] For insurance policies, therefore, it may or may not be advantageous to enter detailed negotiations. Bigelow suggests that the corporation first determine and specify to the insurance company exactly what it wants, and then let the insurer come back with, in effect, a "counter-offer."[319]

Recent court cases involving corporate responsibility for toxic-waste cleanups, for example, have tended to hold the corporate policyholder, rather than its insurer, responsible. These decisions have tended to "turn on narrow issues of contract and insurance law," states Amy Docker. She continues:

---

[317] Elsner, David, "No-Call Toll Mounts in West Suburbs," Chicago Tribune, May 13, 1988.

[318] Bigelow interview.

[319] Ibid.

> The decisions are resting less on good policy than on legal niceties, such as interpretations of the precise wording of the insurance agreements and legal precedents that took shape long before the term toxic waste was coined.[320]

The protection for information resources that may be obtained through insurance is, as with the other approaches to protection, imperfect. Provided the points noted above are considered, insurance may nevertheless offer valuable auxiliary protection, and in some cases and corporate situations may offer the most cost-effective protection available.

Marr Haack offers an observation on business averages spent on insurance for information resources, which may be useful in planning corporate coverage. He suggests that one-fourth to one-half of 1 percent of an asset's value is the average spent on annual premiums. He has seen, depending on circumstances, premiums as high as 2 percent, but suggests that a prudent expenditure is almost always below 1 percent.[321]

An effective corporate policy for the protection of information resources will be enhanced if all available protection approaches – including reduction or elimination of the information resource, education, use of contract services, disaster recovery, an aggressive legal posture, published procedures, codes and policies, technical measures, and insurance – are weighed against the value and vulnerability of those resources. None is perfect or self-sufficient, yet all have much to offer for careful consideration.

---

[320] Docker, Amy, "Corporate Polluters Paying the Price: More Rulings Favor Insurers in Toxic Suits," Wall Street Journal, August 1, 1989, B1.

[321] Haack interview.

CHAPTER SIX

CONCLUDING COMMENTS

This report has offered a framework and a detailed examination of important considerations corporations can use in thinking about, and in developing, policies to protect information resources.

If there are any underlying principles to the overall discussion, they are as follows:

- Information resources are both valuable and vulnerable.
- Many consultants, vendors, and other interested parties are eager to offer corporations "solutions" to individual parts of the overall problem; yet, it is increasingly difficult to grasp the entire issue and to approach it with a reasonable sense of balance.
- Perfect security is neither obtainable nor cost-effective; however, good security is both obtainable and cost-effective.
- Even if little or no specific action is taken to protect corporate information resources, it is useful and prudent to carefully consider corporate policies in this area, and to document what actions were taken and why – or why actions were not taken.
- Those who pretend to offer certainty or "hard" quantitative data on security issues, especially dealing with the valuation of information resources, should be considered with a healthy dose of skepticism.
- A combination of protective measures is almost always preferable to reliance on a single approach.
- Although the security of information resources may have been a "back-burner" issue in the past (to be entrusted to lower-level management), it is no longer prudent for top management to either ignore or delegate the essentials of this issue.

Many different, and informed, views propose what the future will bring to bear on the protection of corporate information resources. Some say that computer "hacking" will increase; others argue that it is on the decrease. Some say that corporate liability in this area will increase; others say that the heyday of compensatory and punitive damages in tort law are over. Some say that technical security measures

will become so widespread that most accidental errors and crimes will be a thing of the past; others suggest that the opportunities for abuse and crime will continue to increase. Some say that due to the general uncertainties, insurance approaches will be in retreat; others argue that precisely due to those uncertainties, insurance will become increasingly attractive. Some suggest that the government will step in; others suggest that the government has no place in the security of private systems.

This author believes plenty of room is available for reasonable people to disagree about these and other questions, which are central or tangential to the issues discussed in this report. However, one certainty exists: information resources are important. The security of these resources is important. And as more "value" moves into these systems, the question, Do we need to protect them? will move closer to the center of corporate decision making.

APPENDIX A

CHECKLISTS FOR IDENTIFICATION OF INFORMATION RESOURCES

Although chapter 2 of this report contains several approaches for corporations to identify their information resources, it may be useful to identify such systems from a checklist. Accordingly, two items are offered here: a representative list of information resources emphasizing communications and computer systems, and a broader listing from the Harvard map of the "information business."

REPRESENTATIVE LIST OF INFORMATION RESOURCES

Automated manufacturing systems
Automated teller machines

Bypass communications systems

CAD/CAM terminals and workstations
Calculators
Cellular radios
Commercial computer databases and services
Communications systems (all types)
Computers (from micros to mainframes)
Computer workstations

Databases
Decision support systems
Desktop publishing systems
Dictating equipment
Distributed information systems

Electronic bulletin boards
Electronic databases
Electronic Data Interchange systems
Electronic funds transfer systems
Electronic mail
Electronic memorandum devices
Emergency communications and computing systems
Executive Information Systems

FAX equipment

Idea processing systems
Integrated Services Digital Network (ISDN) services & equipment

Local Area Networks

Microwave communications systems
Modems
Multiuser databases

Paging systems
PBX/PABX equipment
Personal computers
Point-of-sale accounting and inventory systems

Radios (all types)

Satellite communications systems
Software (all types)
Spreadsheets
Switching equipment

Telephones

Video-teleconferencing systems
Videotext systems
Visual aids and graphics systems
Voice mail

Wide area networks
Word processors

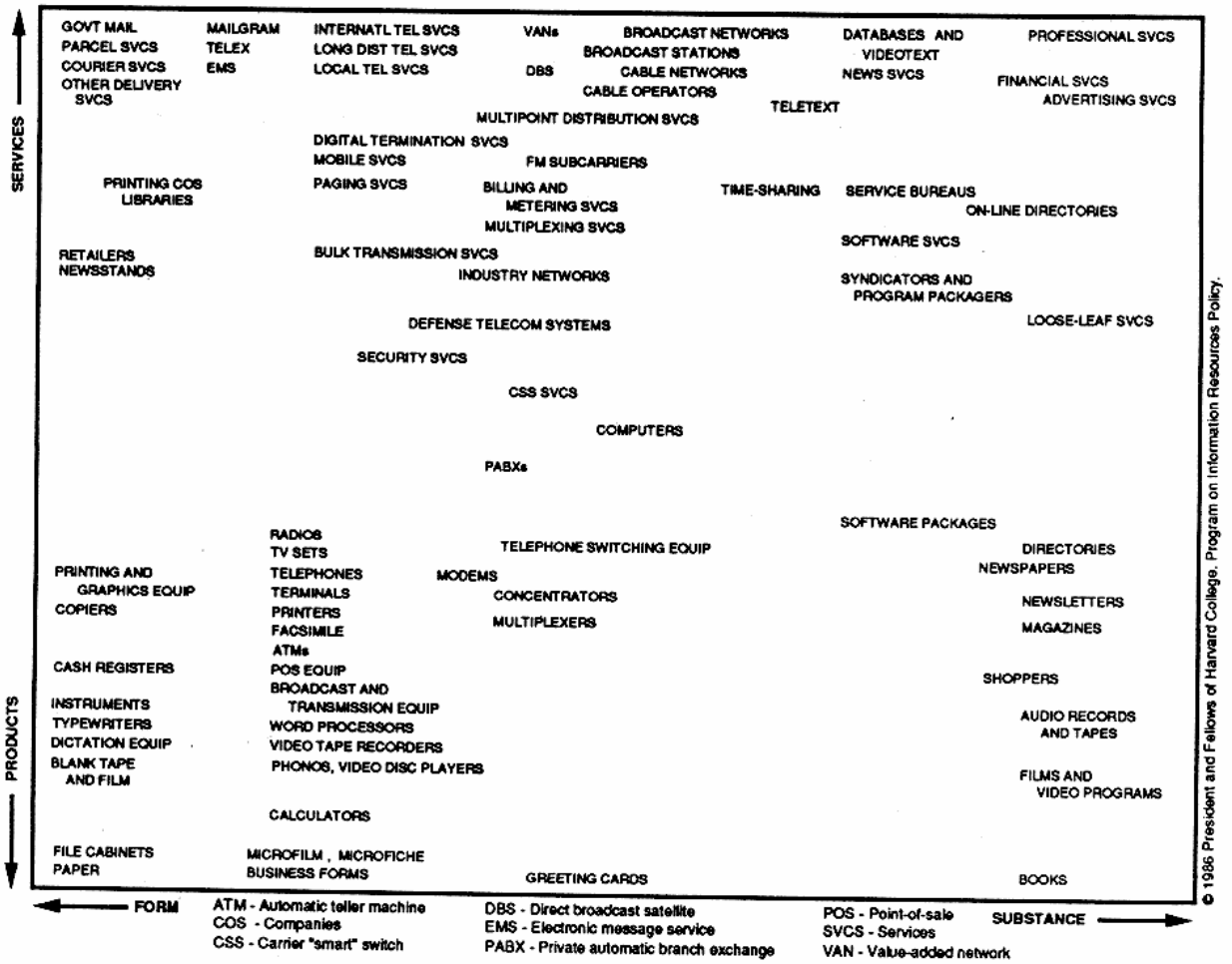

Figure A-1

The Information Business Map

APPENDIX B

COMPUTER-RELATED LEGAL REFERENCES

Listed below are references to state and federal laws that are relevant to the discussions in chapter 3 of this report. Most of the state law citations are based on Ronald J. Palenski's *Compendium of State and Federal Computer Crime Laws*, prepared for ADAPSO in March 1989. Laws added to the books from early to mid-1989 have been included.

STATE LAWS

Ala. Code sections 13A-8-100 to -103 (Supp. 1988)
Alaska Stat. sections 11.46.740 to -.990 (Supp. 1988)
Ark. Stat. Ann. sections 5-41-101 to -107 (1987)
Ariz. Rev. Stat. Ann sections 13-2301 and -2316 (1978 and Supp. 1988)

Cal. Penal Code section 502 (West 1988)
Colo. Rev. Stat. sections 18-5.5-101, -102 (1986)
Conn. Gen. Stat. sections 53a-250 to -261 (1985)

Del. Code. Ann. tit. 11, sections 931 to 939 (1987)

Fla. Stat. Ann. sections 815.01 to -.07 (1981)

Ga. Code Ann. sections 16-9-90 to -95 (1988)

Haw. Rev. Stat. sections 708-890 to -896 (1985)

Idaho Code sections 18-2201, -2202 (1987)
Ill. Crim. Code sections 16D-1 to -7 (Smith Hurd Supp. 1988)
Ind. Code Ann. sections 35-43-1-4 to -3 (Burns Supp. 1988)
Iowa Code Ann. section 167 (West Supp. 1988)

Kan. Stat. Ann. section 21-3755 (1988)
Ky. Rev. Stat. Ann. sections 434.840 to .860 (1985)

La. Rev. Stat. Ann. sections 73.1 to -.5 (West 1986, Supp. 1989)

Me. Rev. Stat. Ann. tit. 17-A, section 357 (1983)
Md. Code Ann. art. 27, section 146
Mass. Gen Laws Ann. ch. 266, section 30 (West Supp. 1988)
Mich. Stat. Ann. section 28.529
Minn. Stat. Ann. sections 609.87 to -.89 (West 1989)
Miss. Code Ann. sections 97-45-1 to -13 (Supp. 1988)
Mo. Stat. Ann. sections 569.093 to -.120 (Vernon Supp. 1989)
Mont. Code Ann. section 45-2-101, sections 45-6-310 to -311 (1987)

Neb. Rev. Stat. sections 28-1343 to -1348 (1985)
Nev. Rev. Stat. sections 205.473 to -.477 (1987)
N.H. Rev. Stat. Ann. sections 638.16 to -.19 (1986)
N.J. Stat. Ann. sections 2A:38A-1 to -6 (1987)
N.M. Stat. Ann. sections 30-16A-1 to -4 (1984)
N.Y. Penal Law sections 156.00 to -.50
N.C. Genl. Stat. sections 14-453 to -456 (1986)
N.D. Cent. Code sections 12.1-06.1-01(3) to -08 (Supp. 1987)

Ohio Rev. Code Ann. sections 2901.01, 2913.01 to -.04 (Supp. 1987)
Okla. Stat. Ann. tit. 21 sections 1124, 1951 to 1956 (West. Supp. 1989)
Ore. Rev. Stat. Ann. sections 164.125 to -.377 (Supp. 1987)

Pa. Stat. Ann. tit. 181 section 3933 (Purdon Supp. 1988)

R.I. Gen. Laws sections 11-52-1 to -5 (1981 and Supp. 1988)

S.C. Code Ann. sections 16-16-10 to -40 (1985)
S.D. Codified Laws Ann. sections 43-43B-1 to -8 (Supp. 1984)

Tenn. Code Ann. sections 39-3-1401 to -1406 (Supp. 1988)
Tex. Penal Code Ann. sections 33.01 to -.05 (Vernon 1989)

Utah Code Ann. sections 76-6-702 to -705 (Supp. 1988)

Va. Code sections 18.2-152.1 to -152.14 (1988)

Wash. Rev. Code Ann. sections 9A.48.100, 9A.52.110 to -.130 (Supp. 1989)
W. Va. Code sections 61-3C-1 to -21
Wis. Stat. Ann. section 943.70 (West Supp. 1988)
Wyo. Stat. sections 6-3-501 to -505 (Supp. 1988)

FEDERAL LAWS

Bank Secrecy Act, 12 U.S.C. sections 1730d, 1829b, 1951-1959 (PL 91-508)(1970)

Computer Fraud and Abuse Act, 18 U.S.C. section 1030 (PL 98-473, 1984, as amended by PL 99-474, 1986)

Credit Card Fraud Act of 1984, 98 Stat. 2183 (PL 98-473)

Domestic and Foreign Investment Improved Disclosure Act of 1977, 91 Stat. 1498 (PL 95-213)

Electronic Communications Privacy Act, 18 U.S.C. section 2510 (PL 99-508)

Fair Credit Reporting Act, 15 U.S.C. section 1681 (PL 90-321)(1971)

Family Education and Privacy Rights Act, 20 U.S.C. section 1232g (PL 93-380)(1974)

Foreign Corrupt Practices Act of 1977, 15 U.S.C. section 78; 91 Stat. 1494 (PL 95-213)

Right to Financial Privacy Act, 12 U.S.C. section 3401 et seq. (1978)

Securities Act of 1933, 15 U.S.C. section 77a et seq.

Securities Acts Amendments of 1964, 78 Stat. 565 (Section 1 of PL 88-467)

Securities Acts Amendments of 1975, 89 Stat. 97 (Section 1 of PL 94-29)

Securities Exchange Act of 1934, 15 U.S.C. section 78

Unlisted Securities Trading Act of 1936, 49 Stat. 1375

Video Privacy Protection Act of 1988, 100 Stat. 1860 (PL 99-508)

Wire Fraud Law, 18 U.S.C. section 1343

GLOSSARY*

ADP	Automatic Data Processing
AIDS	Acquired Immune Deficiency Syndrome
ATM	Automated Teller Machine
Audit Trail	A chronological record of system activities that is sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results. Basically, a way to track down events after the fact.
Authentication	The process of verifying with confidence that a person or piece of data is who or what it purports to be
Biometrics	The science of measuring biological factors, typically for identification purposes; for example, a fingerprint is a biometric
Cellular Radio	An area-wide system in which a geographic area is divided into "cells," and radio communications are automatically monitored and switched between and among cells
CEO	Chief Executive Officer
Computer Abuse	Activity which involves the use of, or attack on, computer systems, but which is not clearly or explicitly against the law
Computer Crime	Criminal activity which involves the use of, or attack on, computer systems
COO	Chief Operating Officer
CRS	Computerized Reservation System
CRT	Cathode Ray Tube, an electronic device for displaying information that is similar to a television tube and screen
D&O	Directors and Officers (insurance)
DC	Direct current, in contrast to alternating current (AC)

---

* Definitions in this glossary are as understood and used by the author solely for the purposes of this paper.

DEA	Data Envelopment Analysis, a scheme for valuing information technologies developed by Robert Kauffman and Charles Kriebel
Degauss	To demagnetize a magnetic media, such as a computer floppy disk
DIS	Defense Investigative Service
E&O	Errors and Omissions (insurance)
EAP	Employee Assistance Program, a formal program to help employees with personal problems
EDI	Electronic Data Interchange
EDP	Electronic Data Processing
EE-PROM	An electrically erasable, programmable, read-only memory device
EFT	Electronic Funds Transfer
EIS	Executive Information Systems, various communications and computer systems designed to support executive decision making
E-MAIL	Electronic Mail, refers to a computer based system on which messages may be sent, stored, and read by way of a computer terminal
Encryption	The scrambling of ordinary voice or data to make it unintelligible to anyone who is not authorized to read or receive the information
EPDP	Executive Planning for Data Processing, an IBM proprietary system for estimating the value of an need for data processing support
FAX	Facsimile, a way of sending pictures of documents or photographs by machine. The device first scans the document and then digitizes the information to be sent by way of a transmission media, such as a telephone line.
FBI	Federal Bureau of Investigation
FCPA	Foreign Corrupt Practices Act
FIPS	Federal Information Processing Standards, guidelines published by the National Institute of Standards and Technology (NIST); formerly the National Bureau of Standards (NBS)

FTC	Federal Trade Commission
GAAS	Generally Accepted Auditing (or Accounting) Standards
GAO	General Accounting Office
GSA	U.S. General Services Administration
ICIT	International Center for Information Technologies
ID	Identification
IT	Information Technologies
ITT	International Telephone and Telegraphic Co.
JPL	Jet Propulsion Laboratory
LAN	Local Area Network
Macro	In software, a bundled command that performs a complex sequence of events, such as logging on to a computer network, with a single command
MIS	Management Information Systems
NBS	National Bureau of Standards (now the National Institute of Standards and Technology)
NCSC	National Computer Security Center, part of NSA
NIST	National Institute of Standards and Technology, part of the Department of Commerce; formerly the National Bureau ofStandards (NBS)
Non-Compete Agreement	An agreement between an employee and employer which restricts the competitive activity of the employee after he or she leaves the company
NPV	Net Present Value
NSA	National Security Agency
OCC	Office of the Comptroller of the Currency
OMB	Office of Management and Budget
OSHA	Occupational Safety and Health Administration
PBX	Private Branch Exchange, a local telephone switch, usually contained on office premises
PC	Personal Computer

PIN	Personal Identification Number
R&D	Research and Development
ROA	Return-on-Assets
ROI	Return-on-Investment
SABRE	Semi-Automatic Business-Related Environment, the American Airlines' computerized reservation system
SEC	Securities Exchange Commission
SYSOP	A System Operator, typically controlling a computer network
VOICE MAIL	A network system in which voice messages may be recorded, and accessed from a remote location
VP	Vice-president
YMCA	Young Men's Christian Association