Threats to Information Systems: Today's Reality, Yesterday's Understanding

By: **Karen D. Loch**
Department of Decision Sciences
Georgia State University
Atlanta, Georgia 30303 U.S.A.

Houston H. Carr
Department of Management
Auburn University
Auburn University, Alabama
36849-5241 U.S.A.

Merrill E. Warkentin
Department of Computer Information Systems
Bryant College
1150 Douglas Pike
Smithfield, Rhode Island
02917-1284 U.S.A.

Abstract

Information systems security remains high on the list of key issues facing information systems executives. Traditional concerns range from forced entry into computer and storage rooms to destruction by fire, earthquake, flood, and hurricane. Recent attention focuses on protecting information systems and data from accidental or intentional unauthorized access, disclosure, modification, or destruction. The consequences of these events can range from degraded or disrupted service to customers to corporate failure. This article reports on a study investigating MIS executives' concern about a variety of threats. A relatively new threat, computer viruses, was found to be a particular concern. The results highlight a gap between the use of modern technology and the understanding of the security implications inherent in its use. Many of responding information systems managers have migrated their organizations into the highly interconnected environment of modern technology but continue to view threats from a perspective of a pre-connectivity era. They expose their firms to unfamiliar risks of which they are unaware, refuse to acknowledge, or are often poorly equipped to manage.

Keywords: Threats, information systems security, computer viruses, computer security, computer laws, information resources management

ACM Categories: K.4.2, K.5.2, K.6.m

Introduction

Many organizations have become so dependent on computer-based and telecommunications-intensive information systems that disruptions of either may cause outcomes ranging from inconvenience to catastrophe (Meall, 1989). Our reliance on computer and telecommunications systems has redefined corporate risk. Management now recognizes that threats to continuing operations include technological issues seldom previously considered (Szuprowicz, 1988). A recent survey of U.S. insurance companies is illustrative. The study found that 90 percent of these firms, which are dependent upon data processing systems, would fail after a significant loss or disruption of the EDP facility (Carter, 1988). Protecting the corporation's information system and data warrants management's attention.

Management's concern with information systems security has changed over recent years. In 1981 it ranked as the 14th most important information management topic (Ball and Harris, 1982). By 1985, it had moved to fifth place (Hartog and Herbert, 1986), but a 1986 study (Brancheau and Wetherbe, 1987) reported security in 18th place. By 1989, the issue had dropped to 19th place (Neiderman, et al., 1991), seeming to indicate that the MIS executives believed either that security was less of an issue, or they had implemented greater control. However, a major study conducted during 1989-1990 by the National Research Council (1991) concludes that, "the state of computer security in the USA is a mess."

Considerably less information is available regarding information systems management's perspective on specific risks. We investigated MIS executives' concern for 12 threats, including a new and special threat, computer viruses. We also evaluated MIS executives' perception of threats for microcomputer, mainframe computer, and network environments. This article reports our results.

Evolution of Computer Security

Security once meant safe storage of materials, equipment, and money. Today the primary threat is to corporate data. The computing environment was historically controlled by a few knowledgeable professionals in a centralized batch processing mode. Physical security was of paramount importance. Today, almost unlimited access by a large, knowledgeable community of end users from desktop, dial-in, and network facilities creates a new and extremely vulnerable environment. The threats to data and system security include natural and man-made disasters, errors by loyal employees, and the overt acts of competitors, hackers, and creators of computer viruses. The results of and reactions to the Hinsdale fire, Hurricane Hugo, the San Francisco earthquake, the Chicago flood, the Internet worm, and the arrest of a national hacker ring reinforce these concerns and underline the seriousness of the situation.

We watched on television the awesome force of Hurricane Hugo as it destroyed power and telecommunications lines, equipment, homes and businesses. In Hinsdale, Illinois, many residents and organizations remember the fire that left them without telephone service for days, weeks, and even months. The San Francisco earthquake began by shaking the stands at Candlestick Park and ended tumbling buildings, bridges, and power transmission facilities. The muddy flood waters in Chicago reminded us that computer rooms are much too important for organizations to be located in basements and other low-lying areas. When Robert Morris planted a worm in the Internet networks he apparently did not mean to halt the productive work of thousands of computers and its attached networks, but it happened. And finally, hackers, whether they are out for a joy ride on your network or intend to steal processing and network paths or destroy data, continue to do their devilish deeds. We doubt the artist Michelangelo ever envisioned the anniversary of his birth being used as an excuse to overtly attempt to destroy all of the data on as many small computers as inhumanly possible.

"The ultimate aim of any computer security policy must be to protect the integrity, availability, and confidentiality of the electronic data held within the system" (Smith, 1989). We protect our systems and data from the *risk of change or destruction,* a risk due to the presence of *threats* (McGaughey, et al., 1991). We tend to equate risk with something done to us. Natural disasters disrupt our power, our ability to produce, or our transportation capability. Less obvious is the risk we create in our actions, such as the installation of a new computer-based system, distribution of our processing and data storage across a country or world, or, as in the case of the banking industry, the movement from batch processing to telecommunications intensive real-time online processing.

Risk, according to the dictionary, is "the possibility of loss or injury" and "the probability of such loss" (Merriam-Webster, 1989). Risk includes threats, resources, modifying factors, and consequences (Crockford, 1980). The components of risk are illustrated in Figure 1. Multiple forces exert influence on the organization; *threats* are a broad range of forces capable of producing adverse consequences. *Resources* consist of the assets, people, or earnings potentially affected by threats. *Modifying factors* are the internal and external factors that influence the probability of a threat becoming a reality or the severity of consequences when the threat does become a reality. *Consequences* are the ways a realized threat impacts the resources (Crockford, 1980).

An alternative threat model includes sources, motives, acts, results, and losses (Parker 1981). Here the concept of risk is included within the losses category. Similar lists have been proposed by others (Busch, 1978; Courtney, 1981; Fisher, 1984; Fitzgerald, 1978; Mair, et al., 1978; Martin, 1973). Contrasting these lists with our focus on threats results in the four-dimensional model for IS security, shown in Figure 2. A list of 12 security threats based on this model is shown in Figure 3. The list is derived from the MIS literature and informal interviews with MIS faculty.

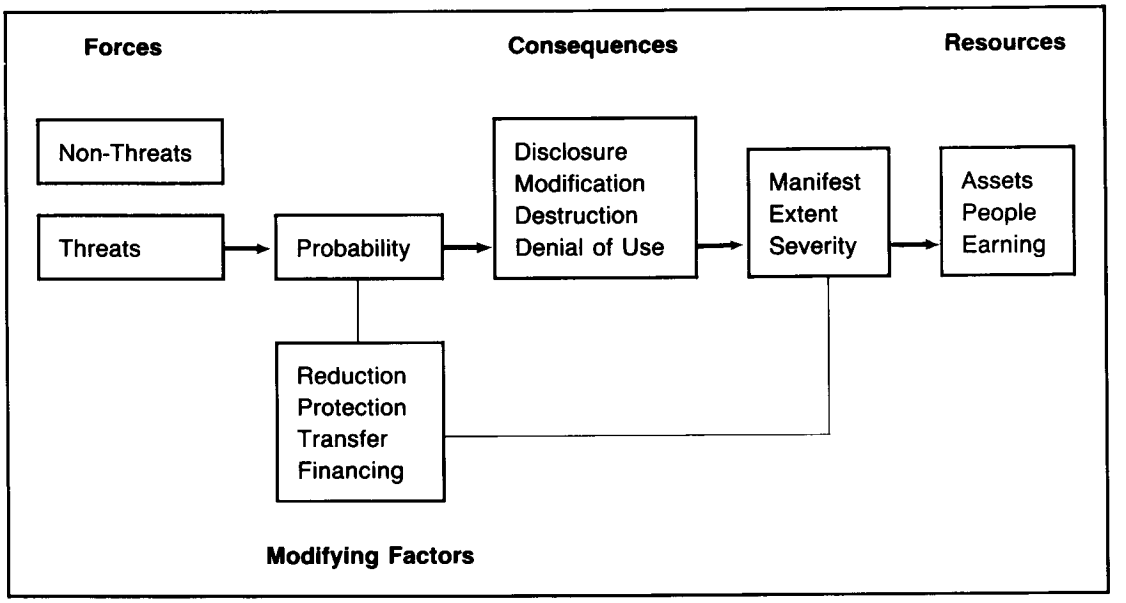

Figure 1. The Components of Risk

Table 1 categorizes these threats by source and perpetrator. Following the model in Figure 2, a threat can be internal to the organization as the result of employee action or failure of an organizational process, or from the external environment. The most obvious external threats to computer systems and the resident data are natural disasters: hurricanes, fires, floods, and earthquakes. Wide use of telecommunications poses a threat of a different type—access to internal data from external sources by competitors and computer hackers. A recent, growing threat is the computer virus (Schweitzer, 1989). First reported in the academic literature in 1987 (Davis and Gantenbein, 1987), viruses have received considerable recent attention (Alexander, 1990a; Baskerville, 1991; Hoffer and Straub, 1989; National Research Council, 1991).

Another dimension of the threat is that of the perpetrator; human versus non-human. For example, many of the threats listed in Figure 3 are the result of human actions. Other are the result of natural, or non-human, events. It can be argued as to whether a virus is the result of human action (its creator) or its own non-human performance. We choose the latter.

Next, actions of the perpetrator may be accidental or intentional, irrespective of the source. Competitors typically would be interested in information access, while hackers' mischievous behavior may cause the full range of consequences. Also, computer viruses and program problems are differentiated by their creators' intent. Computer viruses are defined as malicious software written to produce an undesirable effect to the system, user, or organization. Program problems are most commonly the result of oversights by the programmers/analysts. All four consequences in Figure 2 are potentially hazardous to the well-being of the organization.

Research Objective and Methodology

This research addressed two questions: (1) What are the threats to information systems and resident data? and (2) Which of these are the most serious threats? We first drew from the literature a list of threats[1] and presented them to IS security executives and consultants. Modifications to the instrument were made based on the reviewers' comments.

[1] In creating the list of threats, we believed that their importance would vary by the three computer environments: microcomputer, mainframe computer, and network systems. We included this distinction because we have not seen it done in other studies.

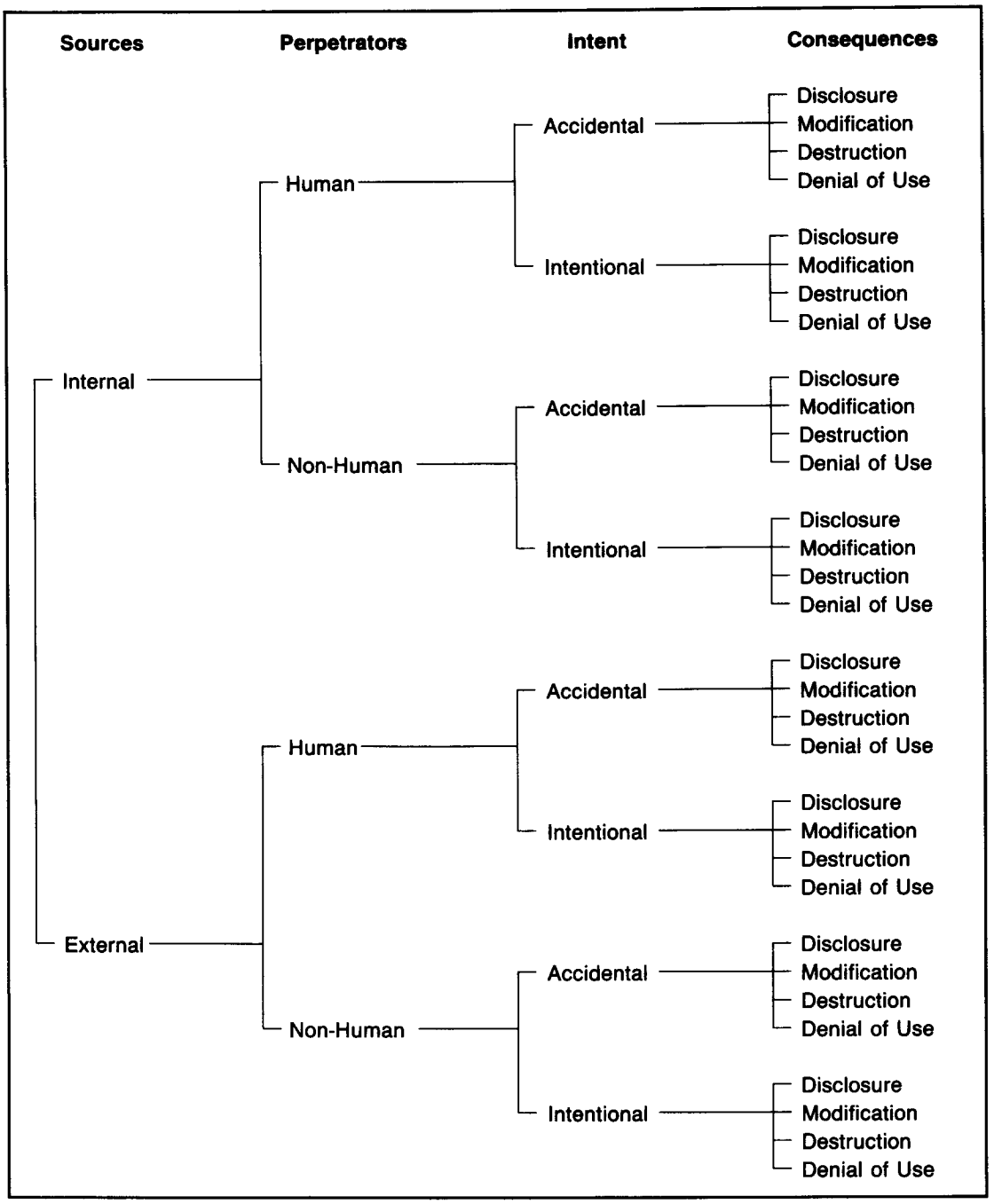

Figure 2. The Four Dimensions of Information Systems Security

Micro-computer	Main-frame	Network	Threats
___	___		Accidental entry of "bad" data by employees
___	___		Intentional entry of "bad" data by employees
___	___		Accidental destruction of data by employees
___	___		Intentional destruction of data by employees
___	___		Unauthorized access to data/system by employees
___	___		Inadequate control over media (disks, tapes)
___	___		Poor control over manual handling of I/O
___	___	___	Access to data/system by outsiders (hackers)
___	___	___	Access to data/system by outsiders (competitors)
___	___	___	Entry into system of computer viruses, worms
___	___	___	Weak, ineffective, inadequate physical control
___	___	___	Natural disaster: fire, flood, loss of power, communications
___	___	___	Other: _____

Figure 3. Threats to Information Systems Security

For a pilot study, we sent questionnaires to MIS directors or MIS security managers in 58 organizations, randomly drawn from the Atlanta, Georgia, entries in the *Directory of Top Computer Executives.*[2] Nineteen responded. The pilot met our initial expectations and required no further modification. We then sent the questionnaire to a random sample of 657 senior MIS managers in the U.S.[3] The organizations were again randomly drawn from the *Directory of Top Computer Executives.* With the help of a follow-up postcard, 131 organizations responded (20.0 percent). Some participants may have elected to not respond due to the sensitive nature of the subject, even though confidentiality was assured. Several respondents refused to respond to selected questions "for security reasons."

Respondents were asked to, "Rank the top three of the following (12) threats to the security of your organization's information system(s), for microcomputers, mainframes, and networks." As shown in Figure 3, the first seven threats were of concern for microcomputer and mainframe computers only, whereas the last five threats were also appropriate for networks. Respondents were allowed to disagree with this classification scheme and to consider all threats appropriate for all environments.[4] Almost without exception, the respondents concurred with the proposed scheme. Respondents were asked to identify the top three threats in each environment.

We used three methods of analysis—weighted votes, the number of first place votes, and unit votes—to describe the overall meaning of including a threat in any of the three positions.[5] Our results are presented in each table.

Analysis

Demographics

Table 2 shows the distribution of the responding organizations by size as measured by number of

[2] *Directory of Top Computer Executives,* (September 1988) East & West Edition, defines the top computer executive as "the person who provides overall planning and direction of all EDP activities" and has an annual DP budget responsibility of $250,000 or more. All companies were in the *Fortune* (April 1989) 1,000 list.

[3] This research was conducted in the spring of 1990.

[4] Space was provided to enter threats not listed, but there was no consistency in the few additions.

[5] *Weighted Votes* are calculated by assigning three points for a first place ranking, two for a second, and one for third. These were then added for each threat by environment. *Number of First Place Votes* are calculated by totaling the number of times each threat is listed as the number one threat. *Unit Votes* are a different perspective of the importance of a threat as shown by the number of respondents who listed the threat in any position (called unit vote). The unit vote shows the total number of responses listing that threat in either first, second, or third place.

Table 1. Source and Perpetrator of Threats to Information Systems Security

Source	Perpetrator	
	Human	Non-Human
Internal Threats	Acts by employees Administrative procedures	Mechanical and electrical failures Program problems
External Threats	Competitors Hackers	Natural disasters Computer viruses

Table 2. Size (in Employees) of Organizations Responding

Size	1–100	101–500	501–1,000	1,001–5,000	Over 5,000	Total
Total Number	26	26	11	49	17	129

employees.[6] The industries responding most were manufacturing (25 percent), financial services (14 percent), education and training (12 percent), and information services (10 percent). The size distribution is fairly even with fewer companies in the 501–1,000 employees category. One-half of the respondents has sales of $100 million or less, and one-half has over $100 million.

Data on DP budgets as a percent of sales/budget was also collected. Forty-seven percent of the organizations reported their DP budget in the 1 percent to 4.99 perecent range. Additionally, 74 respondents provided the size of the IS security budget as a percent of the DP budget. The average IS security budget represents 1.3 percent of the total IS budget and ranged from 0.1 percent to over 10 percent. Thus, the IS security budget often is to the DP budget as the DP budget is to sales.

Connectivity

As illustrated in the movie *War Games,* connectivity increases the risk to a given computer, and to its network, beyond that present with a stand-alone machine. To see the relationship between connectivity and perception of threats, we asked the respondents to note their degree of connectedness (percentage of systems). As shown in Table 3, the microcomputer environment of these organizations was internally connected about one-half of the time but externally connected less, with one in three machines having connectivity. Mainframes are connected internally or externally in two of three installations, connected in both environments one-half of the time, and in a stand-alone configuration in only one in five installations. Thus, most of the responding organizations were familiar with networked environments.

Threats

Overall Risk of Computer Disruption

We asked the participants to, "Please evaluate your organization's overall risk of computer disruption." The overall mean was 3.7 on a scale of one (low risk) to seven (high risk); the standard deviation was 1.2. Respondents were then asked to evaluate their organization's risk of computer disruption by each architectural environment. Table 4 shows the means and standard deviations for the different environments. The network environment was further broken down by whether the organization used networks within their organization, networks connected to the outside world, or both. The microcomputer environment and the external network environment were seen to represent the greatest level of risk. While security experts warn that the greatest threats come from inside the organization (Collins, 1988; Mylott, 1985), the respondents indicated that they

[6] Sales figures were also provided by profit-oriented firms and budget figures were provided by not-for-profit organizations. Size of organization is not shown but compared directly with size by number of employees.

Table 3. Percent of Computer Connectivity

Environment	Stand-Alone (No Connectivity)	Internally Connected	Externally Connected	Internal and External
Microcomputer	37.5%	46.3%	15.0%	23.7%
Mainframe	20.0%	68.6%	61.9%	55.8%

Note: Total percentages exceed 100 percent because organizations reported connectivity levels for all four categories.

perceived a very low level of risk with their internal networks. The range of means between 1.70 and 4.40 is an indication of a low to moderate perceived risk. In other words, the respondents believed they were generally not at risk.

Respondents consistently saw themselves to be at greater risk in the microcomputer environment than in the mainframe environment. Fifty-six percent of the respondents viewed their organization's risk of computer disruption in the microcomputer environment to be moderate/high to high risk (5 to 7 on a seven-point scale). In contrast, 62 percent perceived their organization's risk of computer disruption in the mainframe environment to be low risk (1 to 3 on a seven-point scale) across all types of connectivity. The sensitivity within the microcomputer environment may be in part explained by its recency in comparison to the mainframe environment. Administrative procedures and physical control mechanisms for mainframes are well-understood and in force in most organizations. For microcomputers and related peripherals, however, such controls may be weak or easily ignored.

Our respondents generally believed that external networks represented the greatest risk. Nevertheless, they exhibit a low level of concern. The point of entry to external networks is usually the mainframe system, systems they believe to be relatively secure. In one organization for instance, all communications come into the organization by the mainframe with security password access and call-back modem. This respondent saw little cause for concern.

Table 4. Perceived Risk Level for Computer Disruption, Overall and by Environment (Low Risk = 1; High Risk = 7)

Environments	Mean	Std.
Overall	3.7	1.2
Microcomputer	4.4	1.7
Mainframe	3.5	1.5
Internal Networks	1.7	1.5
External Networks	4.1	1.6

Respondents admitted that there must be more consistent enforcement of what measures and policies are in place in organizations. They evaluated management's commitment to enforcing IS security policies as moderate (mean = 4.4, std. dev. = 1.7; 1 = low commitment, 7 = high commitment). In turn, they believed their current IS policies to be moderately good (mean = 4.6, std. dev. = 1.4; 1 = very poor, 7 = exceptionally good).

Ranking Threats Across Environments

Respondents were asked to, "Rank the top three of the following (12) threats to the security of your organization's information system(s), for microcomputers, mainframes, and networks." The results across methods of analysis shown in Table 5 were highly consistent for the leading threats. Natural disasters and employee accidental actions ranked among the top three threats by all three methods. Using the weighted vote method, natural disasters received 19.8 percent of the possible votes.[7] Natural disasters was displaced in first place by accidental entry of bad data by employee and accidental destruction of data by employee under the first place and unit vote methods respectively.

Tables 5 and 6 show which threats are internal in source and which are external. Table 6 places the threats in the source/perpetrator schema by the weighted vote method. The perpetrator may

[7] One hundred thirty-one respondents could distribute three votes that translate to six weighted votes in each of three environments, for a total of 2,358 weighted votes. Some participants did not cast all votes.

Table 5. Threat Ranking for All Environments

Threats (All Environments)		Weighted Votes Nr.	% Tot	Rank	1st Place Votes Nr.	% Max	Rank	Unit Votes Nr.	% Max	Rank
Natural disasters	E	324	19.8%	1	* 63	16.0%	2	* 159	40.5%	3
Accidental entry bad data by employees	I	270	16.5%	2	+62	23.7%	1	+115	43.9%	2
Accidental destruction data by employees	I	252	15.4%	3	+40	15.3%	3	+130	49.6%	1
Weak/ineffective controls	I	149	9.1%	4	* 24	6.1%	5	* 77	19.6%	5
Entry of computer viruses	E	128	7.8%	5	* 21	5.3%	6	* 68	17.3%	7
Access to system by hackers	E	123	7.5%	6	* 18	4.6%	7	* 66	16.8%	8
Inadequate control over media	I	96	5.9%	7	+17	6.5%	4	+ 51	19.5%	6
Unauthorized access by employees	I	93	5.7%	8	+11	4.2%	8	+ 53	20.2%	4
Poor control of I/O	I	67	4.1%	9	+ 6	2.3%	10	+ 44	16.8%	8
Intentional destruction data by employees	I	58	3.5%	10	+ 7	2.7%	9	+ 33	12.6%	10
Intentional entry bad data by employee	I	36	2.2%	11	+ 4	1.5%	11	+ 22	8.4%	11
Access to system by competitors	E	31	1.9%	12	* 5	1.3%	12	* 16	4.1%	12
Other threats		10	0.6%	13	2	0.5%	13	5	1.3%	13
External/Internal		1637			280			839		

+ Max N = 262; *Max N = 393.

Note: The 131 organizations could cast a maximum of 262 votes for the seven threats listed for microcomputer and mainframe computers-only environments (identified in Table 5 with a +) and a maximum of 393 votes for the five threats in all three environments (identified in Table 5 with an *). By considering the organizations that indicated an awareness of the threat, as a percent of the possible number that could show an interest, a relative standing is achieved.

be human or non-human. External threats received 37.0 percent of the weighted votes and the internal threats received 62.4 percent of the weighted votes, giving internal threats almost a 2 to 1 value over external. These results confirm experts' claims (Collins, 1988) that the greatest threats come from inside the organization.

Ranking of Threats by Environment

Of particular interest were the susceptibility to threats within each of the three computer environments and the importance of each threat within the various environments. We first asked the participants to, "Please distribute 100 points across these three environments to show the seriousness of threats."[8] Table 7 shows the relative risk to all threats by environment, by spreading 100 points. The network environment was noted to be, on average, the least risky environment (with 23.9 of 100 points); however,

[8] The use of the point-spread method, the distribution of a limited amount of points over a field of choices, is referred to as an *ipsative approach*, "in which each value is measured at the expense of the others" (Hicks, 1970). The ipsative approach computes relative scores whereas the weighted method determines a placement vote.

Table 6. Threats to Computer Systems and Data by Weighted Votes

Source	Perpetrator: Human (71.8%)		Perpetrator: Non-Human (27.6%)	
Internal Threats (62.4%)	Accidental entry bad data	(16.5%)		
	Accid. dest. data by employees	(15.4%)		
	Weak/ineffect. physical control	(9.1%)		
	Intent. dest. data by employees	(3.5%)		
	Unauth. access by employees	(5.7%)		
	Intent. entry bad data by employees	(2.2%)		
	Inadequate control over media	(5.9%)		
	Poor control of I/O	(4.1%)		
	TOTAL = (62.4%)			
External Threats (37.0%)	Access by competitors	(1.9%)	Natural disaster	(19.8%)
	Access by hackers	(7.5)	Computer viruses	(7.8%)
	TOTAL = (9.4%)		TOTAL = (27.6%)	

large standard deviations reflect disparity among the respondents. This method provides an indication of the relative level of overall threat to each environment. Table 8 shows the weighted vote results by threat for each environment.

Microcomputer Environment. Four of the five threats leading the list for microcomputers were the same as the leading threats across environments (see Table 5). The ordering, however, differs. Many respondents seemed to believe that data run the same risk of accidental entry and destruction on microcomputers as it does for larger computers. Administrative procedures ranked third and fourth, suggesting that the relatively recent proliferation of microcomputer technology and resulting organizational responsibilities have not been satisfactorily addressed. The concern for computer viruses in a microcomputer-only environment (#6) was not as great as was expected.[9]

Table 7. Risk to All Threats by Environment—Spread of 100 Points Across Three Environments

Environment	Mean	Std. Dev.	Median
Microcomputer	37.9	21.4	40
Mainframe/mini	35.1	22.7	30
Network system	23.9	13.2	30

Mainframe Computer Environment. The top three threats to mainframe computers were the same as for microcomputers, though the threat of natural disasters appears to be of greater concern for the mainframe environment than for microcomputers. The higher ranking of natural disasters and the introduction of the threat of unauthorized access by employees may reflect the growing trend to use mainframes as large data repositories for critical data and expanded access capability.

Network Environment. The threat of natural disasters tops the list for networks, with access to system by hackers ranking second. The threat of hackers ranked significantly lower in the microcomputer (#10) and mainframe (#8) environments. Respondents saw little threat from their employees or competitors. Intentional acts by employees (ranging from 1.6 percent to 5.5 percent of total weighted votes) or competitors conducting industrial espionage (ranging from 0.9 percent to 4.3 percent of total weighted votes) are viewed as small threats.

[9] It was the concern for computer viruses in a *networked* microcomputer environment that raised this threat to fifth place across environments.

Table 8. Threat Ranking for Each Environment (Weighted Vote Method)

Threats (by Environments)		Microcomputers Weighted Votes Nr.	% Tot	Rank	Mainframe Computers Weighted Votes Nr.	% Tot	Rank	Networks Weighted Votes Nr.	% Tot	Rank
Natural disasters	E	74	11.7%	4	135	21.3%	2	115	31.3%	1
Accidental entry bad data by employees	I	112	17.7%	2	158	24.9%	1	-	-	-
Accidental destruction data employees	I	137	21.6%	1	115	18.1%	3	-	-	-
Weak/ineffective controls	I	52	8.2%	5	17	2.7%	9	80	21.7%	3
Entry of computer viruses	E	50	7.9%	6	13	2.0%	11	65	17.7%	4
Access to system by hackers	E	16	2.5%	10	20	3.1%	8	87	23.6%	2
Inadequate control over media	I	80	12.6%	3	16	2.5%	10	-	-	-
Unauthorized access by employees	I	38	6.0%	7	55	8.7%	4	-	-	-
Poor control of I/O	I	31	4.9%	8	36	5.7%	5	-	-	-
Intentional destruction data by employees	I	23	3.6%	9	35	5.5%	6	-	-	-
Intentional entry bad data by employees	I	10	1.6%	11	26	4.1%	7	-	-	-
Access to system by competitors	E	9	1.4%	12	6	0.9%	12	16	4.3%	5
Other threats		2	0.3%	13	3	0.5%	13	5	1.4%	6
External/Internal		634			635			368		

The threat of natural disasters has existed since the introduction of computer information systems, but consequences continue to increase as organizations become more dependent upon the reliable, real-time functioning of their systems and ready access to large databases. A fire that knocked out an electrical substation in lower Manhattan on August 14, 1990, publicly illustrated the financial service industry's vulnerability to natural disasters interrupting telecommunications-intensive systems.

Computer viruses

We were particularly interested in how managers viewed computer viruses relative to other threats. Viruses were ranked as the #4 threat in the network environment and #6 threat in the microcomputer environment. For mainframes, however, viruses were not viewed as an important threat. As one respondent noted, "Viruses are mostly a concern for microcomputer users."

We asked respondents three questions about computer viruses. First, "Has your organization had any verified incidents of computer disruption due to the intrusion of computer viruses or worms?" Twenty-two percent of the respondents reported verified incidents of a computer virus. Not surprisingly, larger companies were more likely to report an incidence. Three industries, education and training, information services, and manufacturing, represented 68 percent of all reported incidents. Education and training led by a significant margin, with 60 percent reporting a verified incident. Thirty-four percent of the IS

firms and 19 percent of the manufacturing firms reported verified virus incidents.

Second, "Please evaluate [on a seven-point scale with 1 = very low and 7 = very high] your organization's risk of computer disruption on your information system due to the intrusion of computer viruses, worms, etc." Seventy-four percent of the respondents replied with a value of three or less; the average response was 2.7. In contrast, they view other organizations' risk to be significantly greater (mean = 4.3). Organizations that had experienced a virus attack saw the threat as greater than those that had not.[10] Nonetheless, in both cases their view of risk was still relatively low.

Third, "The issue of computer viruses is not a major concern in my organization [a seven-point scale with 1 = strongly disagree, 4 = neutral, and 7 = strongly agree]." Overall, the respondents were indifferent about viruses; the median and mean values were 4 and 4.2 respectively. Eighteen percent of the respondents neither agreed nor disagreed with this statement, selecting a value of 4. Those organizations that had *not* experienced a virus incident more strongly disagreed with this statement, indicating a slightly greater concern for computer viruses. In contrast, organizations who reported an incident were evenly divided between moderate and no/low concern. It may be that those who had experienced a virus now felt more comfortable because (1) they had been through the experience, and (2) believed they had addressed their weaknesses in security. Not only do they believe that they are at low risk (mean = 2.68), they also believe that other organizations' risk of computer disruption due to computer viruses (mean = 4.32) is significantly greater than their own ($p = .00001$).

Prevention of Computer Viruses

We then focused on the prevention of computer viruses, asking respondents to rank possible actions designed to prevent infection by computer viruses, worms, etc. Table 9, a list drawn from the MIS literature, shows that passwords, regular backups, and employee education are by far believed to be the most effective preventive measures for viruses. Less than 2 percent of the responding organizations conducted ethics training.

Sanctions for Computer Viruses

It has been estimated (Alexander, 1990a) that businesses report only about 6 percent of criminal acts aimed at their computer systems for fear that the publicity will hurt business or attract copycat crooks. Despite our guarantee of anonymity and confidentiality, several respondents refused to answer specific questions "for security reasons"; others questioned our promise of anonymity. Twenty-two percent of the respondents reported a verified computer virus incident; 50 percent of those could identify the source of the virus. Only four companies reported taking action against the responsible party. One company took legal action, two companies reprimanded the party, and one took multiple measures: legal, reprimand, and dismissal.

Penalties and laws

To determine the respondents' view of the severity of disruptive actions, we asked about the desirable level of penalties for unauthorized access, the destruction of data through direct manipulation, and the destruction of data by a virus. The penalties ranged from a warning (1), to a misdemeanor (4), to a felony charge (7) on a one-to-seven-point scale. The respondents did differentiate between the seriousness of the actions. Only 55 percent were willing to invoke harsh penalties (6 or 7) for unauthorized access, whereas 86.5 percent believed destruction of data whether by manipulation or by a computer virus warranted harsh penalties. In general, unauthorized access is viewed as less serious than the overt, malicious actions of data manipulation and computer viruses.

Respondents were also asked if there was a need for federal and state computer security laws. Their responses were significantly correlated with penalties for all three actions described above. The respondents generally felt that federal computer security laws were more necessary than computer laws at the state level. Sixty percent of the respondents did not know whether their state had laws about computer security; 14 percent said that there were no state laws in their state. Respondents were apparently poorly informed because 48 states have enacted laws dealing with computer crime and the other two

[10] A T-test of these data showed significant differences ($p = 0.02$); mean for no incident = 2.47; mean for incident = 3.42.

Table 9. Ranking of Preventive Measures Against Computer Viruses

Virus Infection Preventive Measures	Weighted Votes			Unit Votes
	Votes	Mean	Std. Dev.	
Use of passwords	136	2.34	0.78	58
Backup procedures schedules	84	1.83	0.71	46
Employee education	75	2.27	0.84	33
Consistent security policies	57	1.97	0.91	29
Company provided software only	50	2.08	0.83	24
Use of virus scanning software	42	1.91	0.81	22
Audit procedures strengthened	42	2.00	0.77	21
Monitor computer usage	28	1.56	0.70	18
Auto terminal/account logoff	24	1.71	0.83	14
Shrinkwrap software only	26	2.00	0.82	13
No outside BBS connections	28	2.55	0.69	11
Publish formal standards	19	1.73	0.79	11
Reporting violations encouraged	19	1.90	0.74	10
Control of workstations	7	1.40	0.55	5
Other	6	2.00	1.00	3
Ethics training	5	1.67	0.58	3

are currently considering such legislation (Alexander, 1990b). Only those respondents who had not experienced a computer virus felt there was no need for federal computer security laws.

Summary and Conclusions

Modern organizations increasingly will rely on telecommunications to extend their traditional systems' boundaries to share information and other resources. Placing systems and data in remote locations and accessing them via telecommunications can define business, competition, and security. Organizations are so dependent on computer-based and telecommunications-intensive information systems that they may not survive a significant disruption of either capability. This research captures the views of MIS management about threats to information systems and data security. Some readers will find many results to be predictable: natural disasters remain a force with which to contend; employees and internal organizational procedures are a greater threat than competitors; and the microcomputer environment is not as secure as the mainframe computer. Other readers may share our surprise by attitudes concerning the newest threat, the computer virus. In brief, these respondents believe themselves to be at low risk from viruses, whether they were in the 22 percent of the sample that experienced one or not, and, simultaneously, believe other organizations are at greater risk than themselves.

The respondents are deeply involved with telecommunications (Table 3), yet they don't seem to connect conceptually the level of connectivity (increased number of points of entry into the system) and level of risk (Table 4). While they did differentiate between stand-alone and connected environments, they viewed their internal networks to be relatively secure (Table 4). Strong evidence supporting that the greatest risk is for employees within the organization (Table 5) suggests that this perception is naive. Furthermore, although they acknowledged the potential risk for external networks, respondents perceived themselves to be at low risk (Table 4). Their low level of concern can be explained by several factors. First, most of their external networks involved mainframe systems, which they believed were secure.[11] Second, informal comments sug-

[11] Some managers may be lured into complacency by the existence of security groups within their organizations. Such an office permits the rest of the organization to abrogate their responsibility for security.

gest that they believe the mainframe environment to be impervious to the threat of computer viruses. This perception also indicates a lack of awareness on their part; mainframe viruses have been documented (Price Waterhouse, 1989; *Virus List Digest,* 1989; 1990).

Although the respondents were all senior MIS managers, they were not familiar with state and federal laws concerning computer crimes. They did have strong opinions as to appropriate penalties for unauthorized access and destruction of data by direct manipulation and use of computer viruses. While some responses were contradictory to their experiences, these managers saw disruption of systems and destruction of data as serious actions warranting serious punishment. Although they were generally cavalier about viruses, they strongly supported the need for laws against destroying data with a computer virus. Ironically, many firms appeared hesitant to apply punishment in practice.

Our findings reveal ironies of computer security. Our respondents seemed well aware of the threats but viewed their risk to be moderately low.[12] They also believed that their employees and competitors operate in good faith; intentional actions were consistently ranked as the least likely threats. Furthermore, they viewed their neighbor to be at greater risk than they were, exhibiting a rather naive belief that bad things only happen to other people.

The growth of connectivity and dispersion of technology within or between organizations will continue. Our results suggest that management needs to (1) become more informed of the potential for security breaches in the mainframe environment and via employees' and competitors' actions; (2) increase their awareness in key areas, such as penalties and laws; and (3) recognize that their overall level of concern for security may underestimate the potential risk inherent in the highly connected environment in which they operate.

References

Alexander, M. "Computer Crime: Ugly Secret for Business," *Computerworld* (24:11), March 12, 1990a, pp. 1, 104.

Alexander, M. "Lax Security Invites Liability Nightmare," *Computerworld* (24:13), March 26, 1990b, pp. 1, 127.

Ball, L. and Harris, R. "SMIS Member: A Membership Analysis," *MIS Quarterly* (6:1), March 1982, pp. 19–38.

Baskerville, R. "Risk Analysis: An Interpretive Feasibility Tool in Justifying Information Systems Security," *European Journal of Information Systems* (1:2), 1991, pp. 121–130.

Brancheau, J.C. and Wetherbe, J.C. "Key Issues in Information Systems Management," *MIS Quarterly* (12:2), March 1987, pp. 23–36.

Busch, J.C., Jr., and Sardinas, J.L., Jr. *Computer Control and Audit: A Total Systems Approach,* John Wiley & Sons, New York, NY, 1978.

Carter, R. "Dependence and Disaster—Recovering from EDP Systems Failure," *Management Services* (UK) (32:12), December 1988, pp. 20–22.

Collins, L.J. "Workers Are Top Threat to Computer Data," *Business Insurance* (22:18), May 2, 1988, p. 60.

Courtney, R.H., Jr. "Security Risk Assessment in Electronic Data Processing Systems," IBM Publication TR21, 700-A, revised March 1981, IBM Corporation, Armonk, NY.

Crockford, N. *An Introduction to Risk Management,* Woodhead-Faulkner Limited, Cambridge, England, 1980.

Davis, F.G.F. and Gantenbein, R.E. "Recovering from a Computer Virus Attack," *Journal of Systems & Software* (7:4), December 1987, pp. 253–258.

Fisher, R.P. *Information Systems Security,* Prentice Hall, Inc., Englewood Cliffs, NJ, 1984.

Fitzgerald, J. "EDP Risk Analysis for Contingency Planning," *EDPACS* (6:2), August 1978, pp. 6–8.

Hartog, C. and Herbert, M. "1985 Opinion Survey of MIS Managers: Key Issues," *MIS Quarterly* (10:4), December 1986, pp. 351–361.

Hicks, L.E. "Some Properties of Ipsative, Normative, and Forced-Choice Normative Measures," *Psychological Bulletin* (74), 1970, pp. 167–184.

Hoffer, J. and Straub, D.W., Jr. "The 9 to 5 Underground: Are You Policing Computer Crimes?" *Sloan Management Review,* Summer 1989, pp. 35–43.

Mair, W.C., Wood, W.R., and Davis, K.W. *Computer Control and Audit* (11A), 1978, p. 363.

[12] See Straub (1990) for a discussion on the seeming contradiction between managers' awareness of or personal experience with certain kinds of system misuse.

Martin, J. *Security, Accuracy and Privacy in Computer Systems,* Prentice-Hall, Inc., Englewood Cliffs, NJ, 1973.

McGaughey, R.E., Carr, H.H., Rainer, R.K., Jr., and Snyder, C.A. "Competitive Advantage and Risk Using Information Technology," working paper, MIS-03, Department of Management, Auburn University, Auburn University, AL, 1991.

Meall, L. "Survival of the Fittest," *Accountancy* (UK) (103:1147), March 1989, pp.140–141.

Merriam-Webster. *Webster's Ninth New Collegiate Dictionary,* G. & C. Merriam Company, Springfield, MA, 1989.

Mylott, T.R., III. "Computer Security and the Threats from Within," *Office* (101:3), March 1985, pp. 45–46, 190.

National Research Council. *Computers at Risk,* National Adacemy Press, Washington, DC, 1991.

Niederman, F., Brancheau, J.C., and Wetherbe, J.C. "Information Systems Management Issues for the 1990s," *MIS Quarterly* (15:4), December 1991, pp. 475–502.

Parker, D.B. *Computer Security Management,* Reston Publishing Co., Reston, VA, 1981.

Price Waterhouse. *The Computer Handbook,* Price Waterhouse, New York, NY, 1989.

Schweitzer, J.A. "Virus: A Strain on the System," *Security Management* (33:3), March 1989, pp. 17A–18A.

Smith, M. "Computer Security—Threats, Vulnerabilities and Countermeasures," *Information Age* (UK) (11:4), October 1989, pp. 205–210.

Straub, D.W., Jr. "Effective IS Security: An Empirical Study," *Information Systems Research* (1:3), September 1990, pp. 255–276.

Szuprowicz, B.O. "Technological Vulnerability: How Serious a Threat to Your Business?" *Canadian Datasystems* (20:10), October 1988, pp. 96–99.

Virus List Digest. "DIR Exec on VM," (2:248, 249), electronic journal accessible at Virus-L@IBM1.cc.lehigh.edu, November 27, 1989.

Virus List Digest. "Documented Mainframe Viral Attacks," (3:114), electronic journal accessible at Virus-L@IBM1.cc.lehigh.edu, June 15, 1990.

About the Authors

Karen D. Loch is assistant professor of decision sciences in the College of Business at Georgia State University in Atlanta, Georgia. She received her Ph.D. in management information systems from the University of Nebraska. She has presented papers at national conferences of Decision Sciences Institute, the Institute of Management Science, and Hawaii International Conference on System Sciences and published in the areas of simulation and management of information resources. She is co-editor of *Global Information Technology Education: Issues and Trends* (Idea Group Publishing, 1992). Her research interests include international management of information technology, telecommunications, and management support systems.

Houston H. Carr is associate professor of management (MIS) and associate director of the Thomas Walter Center for Technology Management at Auburn University, Alabama. Before completing his doctorate in information systems, he spent 21 years in industry, the last nine of which were active in analysis, design, and consulting on computer-based pricing and proposal monitoring systems. His research interests include the information center concept for supporting end-user computing, telecommunications management, and the user-friendliness of computer applications. Dr. Carr has published in *MIS Quarterly, Data Base, Information and Management, Journal of Management Information Systems,* and *Data Management.* He recently published *Managing End User Computing* with Prentice Hall (1988).

Merrill E. Warkentin is associate professor of computer information systems at Bryant College in Smithfield, Rhode Island. Dr. Warkentin's research interests are in the areas of knowledge engineering, computer system security management, and applications of DSS and AI technology. His research has appeared in *Decision Sciences, AI and Medicine, Expert Systems, Agroforestry Systems,* and in several books. He is co-author of *Emerging Information Technologies* (Prentice Hall, 1992) and an associate editor of the new ACM journal *Applied Computing Review.*