Perceived Risks And Threats To Accounting Information Systems

Charles E. Davis, (Charles_Davis@Baylor.edu), Baylor University

Abstract

This study reports survey results from 354 practicing accountants and auditors to obtain an understanding of accountants' AIS security concerns. Management was found to be committed to implementing and enforcing system security policies; however, those policies are sometimes less than adequate. Respondents reported different levels of system security risk and different specific security threats in different hardware environments. This differentiation is particularly important given the increase in geographically dispersed networks and access to external systems through the Internet. Respondents also assessed higher levels of risk to systems employing two emerging technologies -- EDI and client/server technologies.

Introduction

Accounting information systems (AIS) have experienced vast changes in the last thirty years, moving from paper-based journals and ledgers to completely automated, paperless systems. With the proliferation of microcomputers and related accounting software packages such as Peachtree, Profit and QuickBooks, even the smallest company can implement an automated AIS. However, the migration from paper to computer has not been without its difficulties. Each technological advancement is accompanied by a new security issue. In fact, security concerns have been included in the AICPA's list of the top technology issues for the past three years, and were seen as the most important technology issue for 1997 (AICPA 1995, 1996, 1997).

The current level of concern over systems security in general can be gleaned from recent Ernst & Young *Annual Information Security Surveys* (Ernst & Young, 1994, 1995, 1996). These surveys of information systems managers and executives clearly show that information system security continues to be a problem. In 1994, 79% of respondents from companies with more that 2,500 employees indicated that information security risks had increased over the previous five years. In 1996, nearly 80% of the survey respondents had incurred a loss related to information security within the past two years, up from 54% reported in the 1995 survey. However, the majority of these victims could (or would) not estimate the financial amount of that loss.

Loch, Carr and Warkentin (1992) report survey results of senior MIS managers' views of information systems security. They find that

Readers with comments or questions are encouraged to contact the authors via e-mail.

while MIS managers use modern technology, they do not necessarily appreciate the accompanying security implications. For instance, respondents reported that externally networked systems presented the greatest security risk, yet these same respondents reported a low level of concern in this area. The managers also reported a high level of telecommunications use, yet they failed to appreciate that increasing the number of entry points into a system also increases the risk of a security breach. Respondents did, however, recognize that security threats differ by operating environment. Finally, the managers appear to adopt an "it won't happen to me" attitude, in that other companies were more susceptible to security breaches than theirs were.

Part of the problem of inadequate system security may result from a lack of internal control emphasis on the part of IS personnel. MIS personnel are not typically trained as extensively as accountants are in internal control. For instance, Ignozio's (1991) textbook on developing and implementing expert systems does not address the issue of internal control. While he does point out the need to validate the consistency and completeness of the system's rule base, no mention is made of validating data inputs or controlling access to the system itself. Other IS texts, such as Capron's (1986) *Systems Analysis and Design,* do contain a chapter on internal controls; however, these texts tend to focus on general controls, often to the exclusion of the application controls that are so important in assuring accurate input. Typical accounting information systems textbooks (e.g., Bodnar and Hopwood, 1995; Romney, Steinbart and Cushing, 1997; Wilkinson and Cerullo, 1997) spend two to three chapters on internal controls.

While the Ernst & Young surveys report only concerns voiced by information systems management, accountants should share these concerns as they relate to the level of internal control present in the AIS. Through internal control reviews conducted in association with both external and internal audits, accountants examine and gain an understanding of the threats to AIS security. While systems managers are concerned with systems security, they are likely more focused on the operational aspects of the system. Given the emphasis accountants place on internal controls, however, it is likely that they area more concerned with systems security than are systems managers. Little is known, however, about the specifics of these concerns. The purpose of this study is, therefore, to obtain an understanding of accountants' AIS security concerns. Once these concerns are known, accountants and systems managers can collaborate to develop a control environment with which both parties are comfortable.

The remainder of the paper is organized as follows. The research methodology is presented in the next section, followed by the survey findings. The implications of the findings are discussed in the final section.

Research Methodology

The Survey

A survey instrument based on that used by Loch *et al.* (1992) was developed to obtain AIS security data from practicing accountants and auditors.[1] Respondents provided demographic information, information about the level of AIS security at their firm[2], and information about their personal views on AIS security. Based on the results of the Ernst & Young surveys (Ernst & Young, 1994, 1995, 1996) reporting that new technologies are often implemented without adequate system security, respondents were also asked to assess the level of security risk associated with two technologies which are being increasingly employed in AIS -- electronic data interchange (EDI) and client/server architectures. The survey instrument was pretested by 12 members of a local chapter of the Information Systems Audit and Control Association. The pretest resulted in rewording of some questions to enhance comprehension.

The Sample

A random sample of 3,054 members of the Information Systems Audit and Control Association and the American Institute of Certified Public Accountants were mailed the survey instrument.[3] A total of 354 usable responses were received, for a response rate of 11.6%. As shown in Table 1, these respondents represent a broad range of industry and experience. This is in contrast to the Ernst & Young survey which primarily surveyed professionals from large firms. Respondents had an average of 6.9 years experience in their current position and 12.7 years total accounting and auditing experience.

Because of the low response rate, the sample was tested for non-response bias. Oppenheim (1966) suggests the use of late respondents as surrogates for nonrespondents. The response period of approximately 2½ months was divided in half to create early and late responder groups. Data for the two groups was compared using chi square tests and ANOVA. No significant differences between the early and late responder groups were found; therefore, it is assumed that non-response bias is not a problem with the survey data.

Survey Results

Assessment of Firm's System Security Environment

The lack of adequate system security documented in previous studies (Ernst & Young, 1994, 1995, 1996; Loch *et al.*, 1992) has tremendous implications for both external financial reporting and internal decision making. Without adequate security over a system, there can be no assurances as to the quality of the information generated by the system. Thus, suboptimal, and potentially disastrous, decisions may be made because of inaccurate data inputs resulting from inadequate security.

To assess accountants' and auditors' current perception of system security, respondents were asked to rate the degree of top management's commitment to implementing systems security policies and enforcing these policies. As reported in Table 2, responses were recorded on a 7-point Likert scale anchored by 1 = "Very Low Commitment" and 7 = "Very High Commitment". Mean responses were 4.37 and 4.15, respectively. Thus it appears that accountants and auditors perceive a moderate level of management commitment to system security. The adequacy of these policies was rated on a 7-point Likert scale anchored by 1 = "very poor" and 7 = "exceptional", with 4 = "adequate". Apparently, respondents feel that while top management is moderately committed to implementing and enforcing system security policies, the policies are not adequate, as evidenced by the mean response of 3.80. In fact, 41% of the respondents rated existing system security policies as less than adequate.

Hardware Platform Risk Assessment

All hardware platforms are not at equal points in the development of adequate security measures. As technology matures, adequate system security environments also evolve. When mainframes were first introduced, control environments were much less secure than they are today. Similarly, today's newer technologies should be expected to have less secure environments. To assess the degree of system security risk, respondents rated the security risk in several different environments on a seven-point Likert scale anchored by 1 = "No Risk" and 7 = "High Risk", with 4 = "Moderate Risk". As reported in Table 3, accountants and auditors do recognize differing levels of system security risk across different environments. Overall, the AIS security environment is seen as moderately risky (mean = 4.46). The most developed environment, the mainframe, is seen as the least risky in terms of system security (mean = 3.71), while the relatively recent externally-networked microcomputer environment is seen as the riskiest (mean = 5.76).

Hardware platform security risk was also

Table 1
Sample Demographics[a]

Employer Type	
Public Accounting	
Big 6	40
Other national firm	3
Regional firm	12
Local firm	91
Other	3
Total Public Accounting	**149**
Industry	
Manufacturing	30
Banking	53
Insurance	26
Health Care	13
Retail Merchandising	7
Wholesale Merchandising	3
Other	42
Total Industry	**174**
Government	**30**
Total Sample Size	**353**

Professional Certification	
CPA	208
CISA	161
CIA	35
CDP	13
Other	27

Employer Size	**Public Accounting**	**Industry**	**Government**
Number of Accounting Personnel			
1-50	100	64	13
51-100	11	33	5
101-150	4	14	0
151-500	6	8	2
Over 200	28	51	10
Number of IS Specialists			
1-5	110	26	5
6-10	7	12	1
11-15	3	8	1
16-20	5	4	1
Over 20	21	123	22

[a] Totals may not equal 354 respondents due to nonresponse on a particular question.

Table 2
Assessment of Accounting Information System Security Policies[a]

	Number of Respondents[b]						
	Very Low Commitment			**Moderate Commitment**			**Very High Commitment**
	1	2	3	4	5	6	7
The degree of commitment to implementing information system security policies demonstrated by top management is:	18	26	38	97	84	70	17
	Very Low Commitment			**Moderate Commitment**			**Very High Commitment**
	1	2	3	4	5	6	7
The degree of commitment to enforcing information system security policies demonstrated by top management is:	19	30	66	79	86	56	13
	Very Poor			**Adequate**			**Exceptional**
	1	2	3	4	5	6	7
Current information system security policies are:	24	33	86	100	62	40	4

[a] Respondents working in industry responded based on their perception of their firm, while those working in public accounting responded based on their perception of their clients.
[b] Number of respondents may not total to 354 due to nonresponse on a particular question.

Table 3
Assessment of Hardware Platform System Security Risk[a]

	Number of Respondents[b]						
	No Risk			**Moderate Risk**			**High Risk**
	1	2	3	4	5	6	7
Hardware Platform (mean response)							
Overall AIS environment (4.46)	0	13	47	124	112	44	11
Stand-alone microcomputers (4.35)	3	56	54	75	62	63	37
Internally-networked microcomputers (4.78)	0	11	33	103	104	78	23
Externally-networked microcomputers (5.76)	3	8	6	25	77	122	108
Minicomputers (4.22)	6	18	59	130	90	33	11
Mainframes (3.71)	3	65	86	105	51	26	7

[a] Respondents working in industry responded based on their perception of their firm, while those working in public accounting responded based on their perception of their clients.
[b] Number of respondents may not total to 354 due to nonresponse on a particular question.

measured by asking respondents to allocate 100 points across four platforms to indicate the relative seriousness of security threats to AIS, as shown in Table 4. Again, networks, both internal and external, are seen as the hardware environment with greatest risk (mean = 38.96).

Table 4
Allocation of 100 Points Indicating Relative Seriousness of Security Threats

	Microcomputers	Minicomputers	Mainframes	Networks
Mean	24.57	14.67	21.75	38.96
Maximum	100	75	90	85
Minimum	0	0	0	0
Standard Deviation	18.22	11.21	17.17	18.06

Specific Security Threats

Since it was expected that different hardware platforms would be perceived to have different levels of system security risk, respondents were provided a list of possible system security threats and asked to rank the top three threats in each of four hardware platform environments: microcomputers, minicomputers, mainframes, and networks. Respondents were allowed to list and rank additional threats if those included in the list were not complete.[4]

Three methods were used to analyze the ranked responses. First, a "weighted vote" was computed by assigning three points to a first place ranking, two points to a second place ranking and one point to a third place vote. The weighted votes cast by all respondents for each threat were then summed for the total vote. The second method of ranking counted only first place rankings by respondents. The final measure, unit vote, counted a first, second or third place ranking, thus reporting the total number of respondents who included the threat in the top three ranking. Results of the rankings across all hardware platform environments are reported in Table 5. As reported, there is little variation in the rankings across ranking method. Accidental entry of "bad" data by employees is perceived as the greatest threat to system security, followed by unauthorized access to data/systems by employees. The fact that the top three threats involve employees is consistent with previous findings that most computer frauds are committed by employees.

Table 6 presents weighted vote rankings of system security threats by hardware platform environment. Since there was little overall difference between results based on the three ranking methods, "weighted votes" was chosen for this analysis to differentiate between rankings across respondents to capture the perceived relative importance of each threat. As shown, accountants and auditors do recognize that different environments are subject to different security threats, as no single threat is ranked in the top three in all four environments. For instance, accidental destruction of data by employees is the number one threat in the microcomputer environment, yet it is perceived as much less of a threat in the other three environments. Similarly, unauthorized access to data/systems by outsiders, the number one threat in a network environment, does not appear to be perceived as a significant threat in the stand-alone microcomputer environment.

Microcomputer Threats

The primary security threats identified in a microcomputer environment are all a function of employees' careless behaviors: accidental destruction of data, introduction of viruses and accidental entry of "bad" data. This environment affords the greatest degree of direct employee

Table 5
Security Threat Rankings - All Hardware Platforms

	Weighted Votes			1st Place Votes			Unit Votes		
Threats	Number	% of Total	Rank	Number	% of Total	Rank	Number	% of Total	Rank
Accidental entry of "bad" data by employees	563	11.5%	1	120	14.7%	1	248	10.2%	1
Intentional entry of "bad" data by employees	129	2.6%	14	28	3.4%	13	58	2.4%	14
Accidental destruction of data by employees	447	9.1%	3	66	8.1%	4	217	8.9%	3
Intentional destruction of data by employees	128	2.6%	15	26	3.2%	15	58	2.4%	15
Unauthorized access to data/systems by employees	480	9.8%	2	84	10.3%	2	235	9.6%	2
Inadequate control over storage media (i.e., disks, tapes, diskettes)	270	5.5%	10	26	3.2%	14	158	6.5%	9
Poor controls over manual handling of input and output data	202	4.1%	13	32	3.9%	12	111	4.5%	13
Unauthorized access to data/systems by outsiders (i.e., hackers)	390	8.0%	5	59	7.2%	6	190	7.8%	5
Introduction of computer viruses to systems	402	8.2%	4	70	8.6%	3	196	8.0%	4
Weak (ineffective, inadequate) physical access controls permitting unauthorized access to systems	309	6.3%	8	45	5.5%	9	161	6.6%	7
Natural disasters such as fire, flooding, loss of power	233	4.8%	12	35	4.3%	11	134	5.5%	11
Poor segregation of information systems duties (e.g., programming and operations)	347	7.1%	6	60	7.3%	5	171	7.0%	6
Poor segregation of accounting duties (i.e., authorization, recordkeeping and custody)	303	6.2%	9	51	6.2%	8	148	6.1%	10
Employee sharing of passwords	249	5.1%	11	36	4.4%	10	131	5.4%	12
Interception of data transmissions from remote locations	93	1.9%	16	15	1.8%	16	52	2.1%	16
Technology advances faster than control practices	311	6.4%	7	55	6.7%	7	159	6.5%	8
Other	41	0.8%	17	11	1.3%	17	17	0.7%	17

Table 6
Security Threat Weighted Vote Rankings By Hardware Platform

	Microcomputers			Minicomputers			Mainframes			Networks		
Threats	Number	% of Total	Rank	Number	% of Total	Rank	Number	% of Total	Rank	Number	% of Total	Rank
Accidental entry of "bad" data by employees	172	13.3%	3	129	11.7%	1	146	12.3%	1	116	8.8%	5
Intentional entry of "bad" data by employees	36	2.8%	11	30	2.7%	14	35	3.0%	13	28	2.1%	16
Accidental destruction of data by employees	200	15.5%	1	78	7.1%	6	66	5.6%	9	103	7.8%	6
Intentional destruction of data by employees	28	2.2%	14	24	2.2%	15	40	3.4%	11	36	2.7%	13
Unauthorized access to data/systems by employees	82	6.4%	7	124	11.2%	2	121	10.2%	3	153	11.6%	4
Inadequate control over storage media (i.e., disks, tapes, diskettes)	127	9.8%	7	64	5.8%	9	43	3.6%	10	36	2.7%	14
Poor controls over manual handling of input and output data	45	3.5%	10	56	5.1%	11	70	5.9%	8	31	2.4%	15
Unauthorized access to data/systems by outsiders (i.e., hackers)	32	2.5%	12	70	6.4%	7	107	9.0%	5	181	13.8%	1
Introduction of computer viruses to systems	175	13.6%	2	39	3.5%	13	34	2.9%	14	154	11.7%	3
Weak (ineffective, inadequate) physical access controls permitting unauthorized access to systems	119	9.2%	5	80	7.3%	5	40	3.4%	12	70	5.3%	7
Natural disasters such as fire, flooding, loss of power	19	1.5%	15	59	5.4%	10	111	9.4%	4	44	3.3%	11
Poor segregation of information systems duties (e.g., programming and operations)	61	4.7%	9	119	10.8%	3	126	10.6%	2	41	3.1%	12
Poor segregation of accounting duties (i.e., authorization, recordkeeping and custody)	83	6.4%	6	87	7.9%	4	79	6.4%	7	57	4.3%	8
Employee sharing of passwords	31	2.4%	13	70	6.4%	8	98	8.3%	6	50	3.8%	10
Interception of data transmissions from remote locations	2	0.2%	17	15	1.4%	16	25	2.1%	16	51	3.9%	9
Technology advances faster than control practices	71	5.5%	8	52	4.7%	12	27	2.3%	15	161	12.2%	2
Other	7	0.5%	16	7	0.6%	17	21	1.8%	17	6	0.5%	17

access to computer hardware, software and data, thus it is more vulnerable to employee behavior. Coupled with this direct access are the identified problems of inadequate control over storage media and weak physical access controls. It is likely that greater security in this environment could be accomplished through user education without the implementation of complicated procedures.

Minicomputer Threats

The threats in the minicomputer environment differ from those in the microcomputer environment. Primary areas of concern include accidental entry of "bad" data by employees, unauthorized access to data/system by employees and poor segregation of duties, both from a data processing viewpoint and an accounting viewpoint. Improved security in this environment appears to require not only user education, but also policies on compatible job responsibilities and restricted access to systems.

Mainframe Threats

The three main security threats in a mainframe computer environment are the same as those identified for the minicomputer environment, although the rank order differs. The number one perceived threat in a mainframe computer environment is accidental entry of "bad" data by employees. This is surprising given that programs run in a mainframe environment are generally mature and contain many control features designed to prevent erroneous data. Mainframe environments are perceived to suffer from inadequate segregation of duties among system personnel. Again, this is slightly surprising since most firms that run mainframe computers have systems departments large enough to segregate the operations functions from the programming functions. Unauthorized access by employees is the third ranked threat, followed closely by natural disasters. Apparently accountants and auditors are not as concerned about natural disasters as systems personnel, since this was the second ranked threat in the Loch *et al.* (1992) study.

Network Threats

Networked environments were seen as the greatest security risk by the respondents. The primary concern is unauthorized access to data/systems by outsiders, recognizing that interconnectivity through the network greatly increases the number of system access points available to hackers. The second greatest risk was the problem that technology is advancing faster than the development of adequate control techniques. This will continue to be a problem as long as rapid technological advancements are made and companies choose to be on the "bleeding edge" of technology. The third greatest risk, introduction of computer viruses, arises from the use of microcomputers in the network.

Emerging Technologies and Security Threats

As has been mentioned, implementation of new technologies generally increases the system security risk. For example, in a recent survey of CIOs, Deloitte & Touche (1994) found that 54% saw security problems as a significant factor in the pursuit of open systems, a new technology gaining momentum in AIS. To ascertain the degree to which new technologies present increased security risks in AIS, respondents were asked whether their company had implemented EDI or client/server technology, two of the newer technological advances being implemented in AIS environments. If either of these technologies were in use, the respondent then assessed on a seven-point Likert scale anchored by 1 = "not at all" and 7 = "high", with 4 = "moderate" to what degree system security risks had increased from the use of that technology.

Client/server technology is more widespread than EDI, with 64.9% of the respondents indicating some level of use in their AIS. Only 51.6% of the respondents indicated use of EDI in their AIS. As shown in Table 7, both emerging technologies have generally increased the

Table 7
Assessment of Security Risks in Emerging Technologies

	Number of Respondents						
	Not at all			Moderate			High
	1	2	3	4	5	6	7
Increase in AIS security risk from EDI	9	14	25	46	42	30	8
Increase in AIS security risk from client/server	4	7	11	34	76	62	30

AIS security risks. However, client/server technology appears to present more risks than EDI. This is possibly due to the recency of client/server implementations in accounting relative to that of EDI.

Discussion of Findings

This study sheds new light on the perceived threats to AIS security risks. Accountants and auditors felt that management was committed to implementing and enforcing system security policies; however, many felt that those policies were less than adequate. Respondents also reported different levels of system security risk in different hardware environments. Mainframe environments were assessed the lowest level of security risk with externally-networked microcomputers found to be the riskiest environment. Not only did the respondents assess different levels of security risks to the various environments, but the specific security threats also were found to differ by environment. This is particularly important given the increase in geographically dispersed networks and access to external systems through the Internet.

Accountants and auditors also assessed higher levels of risk to systems employing emerging technologies. EDI and client/server technologies were both found to increase the perceived level of security risk. This finding is consistent with that of Deloitte & Touche (1995) in which 43% of CIOs surveyed saw security limitations as a major obstacle to implementing client/server systems, up from 36% in 1993. As the move to rightsize systems increases and client/server systems become more prevalent in accounting, accountants and auditors must recognize the security threats and develop adequate measures to control risk at an acceptable level.

The study is subject to limitations. First, the sample was drawn from the membership roles of two professional associations, the AICPA and the ISACA. While these are the major professional certification bodies in auditing and control of AIS, it is possible that the respondents do not accurately reflect the perceptions of the profession as a whole, particularly in light of the low response rate. Second, responses were personal perceptions of security risk, and as such, may not reflect the actual risk present.

Regardless of these limitations, the study does provide useful information for those accountants and auditors involved in AIS security. With the growing interconnectivity within and between various AIS components, security risks will only increase. Professionals must be aware of and address these security issues as new systems are implemented.

Implications for Future Research

There is much still to be learned about the security environment surrounding accounting information systems. Future research should compare auditors' perceptions of clients' systems security with the perceptions of client systems and internal audit personnel. Such research might identify a "perceptions gap" that could influence auditors' reliance on clients' system security controls. The explosion of the Internet and the prospects of electronic commerce through the Internet raise additional security concerns. Research should explore the vulnerability of accounting information systems to security threats arising through the Internet, such as e-mail type (macro viruses) threats. The survey used in this study did not specifically examine threats of this nature. A final area for future research is in the relationship between firm size and threats to accounting information system security. Once threats are recognized in this environment, adequate security measures can be developed and implemented.🕮

Endnotes

1. A copy of the survey instrument may be obtained from the author.
2. Respondents in public practice provided information about their clients' systems, not about the accounting firm's systems.
3. The author gratefully acknowledges the assistance of the ISACA and AICPA in providing access to their membership, and the financial assistance of the Baylor University Research Committee, Hankamer School of Business and Department of Accounting and Business Law.
4. It was apparent from reviewing the completed surveys that many respondents did not understand the desired response method to this question, even though this had not been a problem in the pretest of the survey instrument. This is possibly due to the fact that the EDP auditors who participated in the pretest were more familiar with the terminology than the average accountant. As a result, responses are not available for the entire sample.

References

1. American Institute of Certified Public Accountants, "AICPA Technology Division Announces Top 15 Technologies for 1995," *AICPA InfoTech Update,* Winter, pp. 10-11, 1995.
2. American Institute of Certified Public Accountants, "Top 15 Technologies CPAs Should Know about in 1996," *Journal of Accountancy,* pp. 25-28, January 1996.
3. American Institute of Certified Public Accountants, "The IT Committees' Top 10 List," *Journal of Accountancy,* pp. 12-13, February 1997.
4. Bodnar, G. H. and W. S. Hopwood, *Accounting Information Systems*, 6th ed. Prentice Hall, Englewood Cliffs, NJ, 1995.
5. Capron, H. L., *Systems Analysis and Design,* The Benjamin/Cummings Publishing Company, Inc., Reading, MA, 1986.
6. Deloitte & Touche LLP, *Leading Trends in Information Services: Information Technology Consulting Services Seventh Annual Survey of North American Chief Information Executives - 1995.*
7. Ernst & Young LLP, *2nd Annual Information Security Survey: Trends, Concerns, and Practices,* 1994.
8. Ernst & Young LLP, *3rd Annual Information Security Survey: Trends, Concerns, and Practices*, 1995.
9. Ernst & Young LLP, *Information Security Survey: Analysis of Trends, Issues, and Practices*, 1996.
10. Ignozio, J. P., *Introduction to Expert Systems: The Development and Implementation of Rule-Based Systems*, McGraw-Hill, Inc., New York, 1991.
11. Loch, K. D., H. H. Carr and M. E. Warkentin, "Threats to Information Systems: Today's' Reality, Yesterday's Understanding," *MIS Quarterly,* pp. 173-186, June 1992.
12. Oppenheim, A. N., *Questionnaire Design and Attitude Measurement*. Basic Books, Inc., New York, 1966.
13. Romney, M. B., P. J. Steinbart, and B. E. Cushing, *Accounting Information Systems*, 7th ed., Addison-Wesley, Reading, MA, 1997.
14. Wilkinson, J. W., and M. J. Cerullo, *Accounting and Information Systems: Essential Concepts and Applications*, 3rd ed.,

John Wiley & Sons, Inc., New York, 1997.