DOCUMENT RESUME

ED 333 898 IR 053 660

AUTHOR	Elliott, Raymond; And Others
TITLE	Information Security in Higher Education. Professional Paper Series, #5.
INSTITUTION	CAUSE, Boulder, Colo.
SPONS AGENCY	Coopers & Lybrand, New York, N.Y.
PUB DATE	91
NOTE	35p.
AVAILABLE FROM	CAUSE, 4840 Pearl East Circle, Suite 302E, Boulder, CO 80301 ($8.00 to individuals at CAUSE member institutions/ organizations, $16.00 to others; orders should be prepaid).
PUB TYPE	Reports - Research/Technical (143) -- Tests/Evaluation Instruments (160)
EDRS PRICE	MF01/PC02 Plus Postage.
DESCRIPTORS	*Academic Freedom; *Access to Information; Administrator Role; *Colleges; Emergency Programs; Higher Education; *Information Technology; Interviews; Microcomputers; *Policy; Surveys; *Technological Advancement; Telecommunications
IDENTIFIERS	*Computer Security; Computer Viruses

ABSTRACT

Intended to generate discussion and motivate proactive intervention in matters of information security, this paper defines and discusses some of the key issues relating to information security on college and university campuses based on in-depth interviews conducted at eight selected higher education institutions of varying size and composition in the spring of 1989. Findings, observations, and suggestions for further research are presented in eight areas: (1) Awareness of Information Security; (2) Information Security Concerns, including confidentiality, telecommunications, microcomputers, business continuity/disaster recovery planning, and physical security); (3) Risk Assessment; (4) Information Security Policies, including microcomputer policies; (5) Security and Control; (6) Information Security Administration; (7) Design, Review, and Testing of Information Security: The Role of Auditors and Consultants; and (8) Information Security Issues for the 1990s, including networks, end-user computing, and pace of technological advances. It is concluded that one of the most difficult challenges information technology managers at colleges and universities face today is finding the correct balance between academic freedom and essential security measures. A copy of the interview guide is appended as well as a profile of Coopers & Lybrand, the corporate sponsor of the study, and an annotated listing of six reports in the Professional Paper Series. (24 additional readings) (BBM)

The Association for the Management of Information Technology in Higher Education

Information Security in Higher Education

by Raymond Elliott, Michael O. Young, Vincent D. Collins, David Frawley, and M. Lewis Temares

Professional Paper Series, #5

Information Security in Higher Education

by
Raymond Elliott, Michael O. Young, Vincent D. Collins,
David Frawley, and M. Lewis Temares

CAUSE
The Association for the Management of
Information Technology in Higher Education

Professional Paper Series, #5

CAUSE appreciates the generous support of Coopers & Lybrand, who funded the publication of this professional paper (see pages 24-25).

Copies of this paper are available to individuals at CAUSE member institutions/ organizations at $8 per copy, to others at $16 per copy. Send pre-paid orders to:

CAUSE
4840 Pearl East Circle, Suite 302E
Boulder, Colorado 80301
Phone: 303-449-4430
Fax: 303-440-0461
E-mail: orders@CAUSE.colorado.edu

About the Authors

Raymond Elliott, CISA, is a partner in Coopers & Lybrand. As the partner responsible for Information Technology Research and Planning in the firm's National Auditing Directorate, his responsibilities include identifying information technology that can be used by field practitioners in the delivery of client services. He also researches trends in information technology to assist the Directorate in assessing their potential impact. Prior to assuming his current position, he was Director of National EDP Development where he was responsible for directing the development of auditing software for time-sharing, mainframe, minicomputer, and microcomputer systems. Mr. Elliott is currently the Chairman of the American Institute of Certified Public Accountants Information Technology Research Subcommittee.

Michael O. Young, CPA, CISA, is a director in Coopers & Lybrand's Information Technology Audit Services group, with responsibility for providing information systems consulting, computer auditing, and security services in the Southeast U.S., Puerto Rico, and Latin America. He has extensive technical experience in hardware and software evaluation and selection, telecommunications configurations, contingency planning, and security reviews. Mr. Young is a frequent speaker on information systems security, computer fraud, and contingency planning.

Vincent D. Collins is a director in Coopers & Lybrand's Information Technology Audit Services group. He directs computer audit services for higher education and the development and presentation of internal training courses on information technology issues in the college and university environment. Mr. Collins is a past Treasurer of Central New York EDPAA, and is a frequent lecturer on EDP Audit, Contingency Planning, and Security Concerns and Techniques.

David Frawley is a technical writer in Coopers & Lybrand's National Auditing Directorate. He is responsible for writing and editing a wide range of internal information technology-related publications.

M. Lewis Temares, Ph.D., is the CIO and Associate Vice President for Information Resources at the University of Miami. He is responsible for computing, telecommunications, planning, institutional research, and the testing center. A past Chair of the CAUSE Board of Directors, Dr. Temares has presented, published, and consulted in the area of management, information systems, planning, and statistics.

Acknowledgements

The authors gratefully acknowledge the cooperation and contribution of the following individuals whom we interviewed as part of our research for this paper:

- Maricopa Community Colleges—Ronald Bleed, Vice Chancellor, Information Technology Services
- Ohio State University—Larry L. Buell, Assistant Vice President of University Systems, and Debbie Rife, Administrator of Data Security
- Swarthmore College—William Connor, Director of System and Network Operations
- University of Miami—Peter Rittner, Manager of Security and Disaster Recovery
- University of North Carolina at Greensboro—Eddy Cheng, Director, Management Information Systems, and Gary M. Grandon, Associate Vice Chancellor, Computing and Information Systems
- University of Southern California—Robin Pearse, Director of Special Projects, and James Pepin, Executive Director, University Computing Services
- Virginia Polytechnic Institute and State University—A. Wayne Donald, Manager, Administrative Systems Planning, Robert C. Heterick, Jr., Vice President for Information Systems; and Michael Williams, Director, Computing Center
- Yale University—Douglas Hawthorne, Director, Administrative Support Services for Development and Alumni Affairs, and Bernard J. Hayden, Director, MIS

A special acknowledgement is made to Peter Rittner, University of Miami, for his excellent contributions to this paper.

TABLE OF CONTENTS

LIST OF EXHIBITS

Introduction

On the evening of November 2, 1988, a computer "worm" program attacked the Internet.[1] The attack continued for several days and infected as many as 6.000 machines. Taking advantage of widely known flaws in software frequently installed on UNIX systems and using a mechanism designed to simplify resource sharing in local area networks, the worm replicated uncontrollably, eventually overwhelming the processing capabilities of many infected machines until they failed completely. The cost of such an attack is difficult to estimate. Thousands of hours of system availability time were lost, and tens of thousands of hours were required to correct problems created by the attack. The intangible effects were possibly even more serious: loss of confidence, a retreat from the productive sharing of resources, and undeserved tarnishing of reputations, to name a few.

The Internet attack was not the first computer virus attack, nor will it be the last. The first documented virus, the Creeper, began to spread in 1970 through the ARPAnet, a national network linking university, military, and corporate computers. The Creeper was relatively harmless, its only function being self-replication. In a more damaging incident, the Christmas Trojan horse infected the BITNET in December 1987, appearing on five continents and seriously disrupting IBM's global electronic mail network for seventy-two hours.[2] The widely publicized AT&T outage in January 1989 was reputedly the result of sabotage. Even the Defense Department's computer security has been successfully breached on more than one occasion. The FBI estimates the average computer crime costs $400,000, and Coopers & Lybrand estimates annual worldwide losses to computer misconduct at $15 billion.

The American Council on Education published a white paper in May 1989 entitled *Computer Viruses, Legal and Policy Issues Facing Colleges and Universities*. The authors of this paper questioned whether colleges and universities were particularly vulnerable to virus attacks. Their answer: "Probably. Institutions of higher learning often have an unusual concentration of people with computer expertise and the freedom and incentive to explore frontier technologies."[3] This observation applies to all security issues. One of the most difficult challenges information technology managers at colleges and universities face is finding the correct balance between academic freedom and essential security measures.

A strong motivation for seeking that balance is the threat of legal liability. Colleges and universities can be held responsible for the irresponsible conduct of their

[1]The "Internet" is the name given to the interconnected networks in the NSFNET, a high-speed electronic network created with support from the National Science Foundation that is made up of a transcontinental backbone of trunk lines connecting a number of regional networks, each of which connects a dozen or more campus-area networks. Information about NSFNET, including guidelines on viruses and protecting information resources, is available by sending an electronic mail message to:

INFO-SERVER@NNSC.NSF.NET
containing the text: Request: NSFNET
Topic: Help

[2]Allen Lundell, *Virus! The Secret World of Computer Invaders that Breed and Destroy* (Chicago: Contemporary Books, 1989).

[3]David R. Johnson, Thomas P. Olson, and David G. Post, *A White Paper on Computer Viruses: Legal and Policy Issues Facing Colleges and Universities* (Washington, D.C.: American Council on Education and United Educators Insurance, March 1989).

students or their employees. In all cases, protection of critical information assets is a fundamental responsibility of information systems organizations. Absolute protection is unrealistic and unnecessary. All security measures impose some inconvenience and inefficiency and involve some overhead. For example, secret passwords need to be remembered, entered to obtain access, and controlled by software which uses system resources. Physical access control systems may require the user to carry a card and certainly require some sort of delay upon entering and sometimes upon exiting. The optimal level of protection is that which is minimally required and it can be difficult to define.

The purpose of this paper is to define and discuss some of the security issues facing higher education today and in the near future. We conducted in-depth interviews at eight colleges and universities of varying size and composition to gain insight about how they perceive and approach their security concerns. We did not consider our survey a scientific sample, nor did we intend to draw broad conclusions from what is not necessarily a representative subset of colleges and universities. We expected to discover some interesting consistencies, however, and we did.

If this paper generates discussion and motivates proactive intervention in matters of information security, it will have accomplished its end. After all, information isn't harmful; it's how we use or misuse it that helps or hurts us. As Dr. Fred Cohen, who formally defined the term "computer virus" while a graduate student at the University of Southern California, said when speaking about computer viruses (as quoted in a May 9, 1988, *Dallas Morning News* article): "Ignorance isn't bliss. It's suicide."

Key Findings

The findings from our campus interviews that we feel best frame and introduce the discussion that follows in the next section are:

- Administrators and operations staff are most aware, and faculty and students are least aware, of information security issues.

- The issues affecting computer operations rank in order of importance as follows:
  - — Confidentiality
  - — Telecommunications
  - — Microcomputers
  - — Contingency Planning/Disaster Recovery
  - — Physical Security

- Because institutions have assessed risk in specific areas of computer operations, senior level administrators do not believe an overall security risk assessment is warranted.

- Not all institutions have developed security policies, and most existing policies do not specifically address microcomputer security.

- Security administration is more often a part-time than a dedicated function.

- Expanded use of networks, end-user computing, and the impact of technological advances on security are seen as the issues most likely to affect information security in the 1990s, with image processing and paperless systems identified as the technologies most likely to affect computer operations in the next decade.

Although not conclusive, our study identifies some key issues relating to information security at colleges and universities. Given the rapid pace of technological change, the decentralization of computing, and the proliferation of computers, networks, and users of varying capabilities in the academic setting, information security is an area of significant importance in higher education.

Observations and Concerns

We were not surprised to discover that the higher education executives and managers we interviewed were very knowledgeable and aware of information security issues. In addition to the issues they identified, we would add some concerns based on our analysis of the findings of our study, our experience in serving institutions of higher learning, and our thoughts about the future of computer use on college campuses.

- We believe that in today's environment security risk assessments should be performed regularly to ensure the adequacy of information security policies and procedures.

- We believe that higher education administrators should give serious consideration to addressing viruses—a relatively new threat—and microcomputer security issues. In our opinion, these issues will become more significant, given the increasing use of networks on college campuses and the increasing number of microcomputer users.

- Given the size, complexity, and importance of the computing environments in institutions of higher education today, we believe that colleges and universities should provide business continuity/disaster recovery plans to protect themselves from worst-case scenarios which will hopefully never occur.

- Although some colleges and universities are hiring risk managers, we believe that more institutions should either assign this responsibility to existing staff with appropriate training or hire outside personnel to carry out this function. Moreover, risk managers' responsibilities should include regularly reviewing their institution's information security policies and procedures. These policies and procedures may need to be updated frequently to accommodate the ever-changing computer environment.

Institutions of higher learning should be alert to possible enhancements in their information security policies and procedures. After the Internet worm incident, Cornell University established an inquiry commission to review its security measures. Their report concluded: "The university can only encourage reasonable behavior. It cannot guarantee that university policies and procedures will be followed."[4]

We conclude this introduction with the same cautionary note. Information security administrators and others in the higher education community need to reassess their information security policies and procedures, increase awareness, and otherwise do as much as possible to protect themselves from computer viruses and other threats and adverse situations. In other words, they should do as much as they can to "encourage reasonable behavior."

[4] *The Computer Worm, A Report to the Provost of Cornell University on an Investigation Conducted by the Commission of Preliminary Inquiry* (Ithaca, N.Y.: Cornell University, 1989). Commission members Ted Eisenberg, David Gries, Juris Hartmanis, Don Holcomb, M. Stuart Lynn (Chair), and Thomas Santoro.

Summary of Findings

After identifying what we believed to be the broad information security issues relevant to computer processing, we organized those issues into an "interview guide" (included in the Appendix) that formed the basis for conducting interviews with the participants in our study.

The study was conducted in the spring of 1989 by visiting the campuses of eight colleges and universities.

- Maricopa Community Colleges
- Ohio State University
- Swarthmore College
- University of Miami
- University of North Carolina at Greensboro
- University of Southern California
- Virginia Polytechnic Institute and State University
- Yale University

On each of these campuses, we interviewed the executive(s) directly responsible for information processing for both academic and administrative computing. Where possible, we also interviewed security administrators or the highest level of executive management involved in computing operations.

Issues were identified, our study was conducted, and findings are herein summarized in eight areas:

- Awareness of Information Security
- Information Security Concerns
- Risk Assessment
- Information Security Policies
- Security and Control
- Information Security Administration
- Design, Review, and Testing Information Security: The Role of Auditors and Consultants
- Information Security Issues for the 1990s.

Within each area, notable findings are presented and related issues that would benefit from further research are identified.

1—Awareness of Information Security

It is arguable that broad-based awareness of security issues is the single most effective means of ensuring information security. The effectiveness of most security measures depends largely on the behavior of the people affected by those measures. For example, an access control system based on secret passwords is effective only if people do not share their passwords.

If people are to be aware of security issues they need to be educated about their institution's security concerns and solutions, and they must understand their role in making security measures effective. Such information helps convince people that security measures are necessary and valuable, even given the inconveniences associated with them. In addition, it is advisable to reinforce institutional security values over time to maintain security awareness.

The colleges and universities we surveyed depend largely on definitions of appropriate conduct (codes of conduct, bylaws, formal security policies, even federal and state laws) to establish information security responsibilities and awareness of those responsibilities. In most instances, mainframe computer privileges are issued only after potential users sign an authorization form containing the conditions under which access is granted. In striking contrast, we found a widespread absence of even such rudimentary measures in the microcomputer environment. For example, only two of

the institutions have a code of conduct for microcomputer use, one of which was described as "inadequate" by the participant who reported it. Overall, we found little evidence of proactive security awareness programs, and participants reported no immediate plans for increasing awareness of information security issues.

An institutional commitment to security awareness must come from top administration. Administrators generally stay informed about pertinent information security issues by relying on senior information systems professionals and internal and external auditors. Administrators are often reactive to information security since they are frequently unable to devote adequate time to such issues. For example, corrective actions frequently result only after an unfavorable comment in the annual audit report, or a highly publicized event like a virus attack.

The Internet worm elicited considerable concern from administrators at the colleges and universities we surveyed. They wanted to know whether their institution had been affected, if their institution had been damaged, and if so, why the attack was not prevented.

Findings and Observations

Participants rated (on a scale of low, medium, and high) their campus administration's and their user groups' awareness of information security issues (including software piracy, copyright violations, unauthorized access, and physical security). Findings included:

- Executive administration at institutions which have a full-time security administrator and a security policy received high ratings for information security awareness, while executive administration at institutions without a full-time security administrator or a security policy received slightly lower to much lower ratings.

- Administrators and operations staff are most aware, and faculty and students are least aware, of information security issues and, similarly, administrative computing personnel were more aware of security issues than those involved in academic computing (see Exhibit 1).

It is not surprising that our survey indicated that a formal security administration function correlates to a higher level of security awareness, since a commitment to security administration indicates an institution's administrative priorities regarding security. Furthermore, institutions having people responsible for reviewing, defining, and enforcing security policies are more likely to recognize the need for programs that consciously maintain and reinforce security awareness than institutions that have not assigned such responsibilities.

Participants discussed how information security awareness is maintained and reinforced for administrative and academic computing activities on their campuses. Among the methods used to maintain awareness are the existence of a security policy, a lab monitoring function, meetings, training, agreements, physical security, and written guidelines (see Exhibit 2).

Participants who gave their institutions' administration and users higher overall awareness ratings used a combination of the following to promote awareness:

- Security Policy
- Lab Monitoring Function
- Physical Security
- Written Guidelines

Exhibit 1
Information Security Awareness Ranking

	INSTITUTIONS REPORTING		
	AWARENESS		
	High	Medium	Low
Executive Administration	3	3	2
Administration	5	3	—
Operations Staff	5	3	—
Faculty	1	2	5
Students	—	—	8

Further Research

It is reasonable to assume that executives who have a higher level of awareness about information security issues are better able to plan, implement, and maintain

information security systems. In fact, our study indicates institutions with the most aware administrators and user groups have a full-time security administrator and a security policy, and use a combination of methods to continually promote awareness.

A more in-depth study of a larger population of institutions might address:

- What is the degree of correlation between the existence of a full-time security administrator and a higher level of awareness about information security issues among administration and users?
- What is the degree of correlation between the existence of a security policy and a higher level of awareness about information security issues among administration and users?

2—Information Security Concerns

Participants discussed the issues affecting their computing operations, and collectively ranked them in order of importance as follows:

- Confidentiality
- Telecommunications
- Microcomputers
- Contingency Planning/Disaster Recovery
- Physical Security

Exhibit 2
Methods Used to Maintain Awareness

	Number of Institutions Reporting
Physical	4
Guidelines	4
Policy	3
Lab Monitoring	3
Training	2
Agreements	2
Meetings	1
No Specific Method	1

The information security concerns of colleges and universities are related to their mission to educate. Institutions typically attempt to strike a balance between academic freedom and information security. However, as one participant said, "The need for academic freedom does not lessen the need for security." Administrators need to protect critical information assets; students value their privacy; and scholars, understandably, want assurances their research data are secured to the degree they desire.

Confidentiality of sensitive information (such as student financial information) is a particularly complex issue, especially in light of legal considerations. The Buckley Amendment places responsibility for extensive and thorough protection of all private information about students and their families squarely on the shoulders of administrators. The consequences of failure to fulfill that responsibility can be very serious, both financially and in terms of public perceptions.[5]

Telecommunications technology, particularly in networks, is a source of rapidly emerging security issues. While providing the benefits of global access, telecommunications bridges within and between colleges and universities provide ample opportunities to compromise security measures. Interconnecting networks and the transport of data across those connections have created an environment so complex and active it is difficult to address all the security needs adequately. The effectiveness of the Internet worm illustrates such vulnerability.

Microcomputers at the institutions we surveyed were also a source of security concern, primarily due to the ease of physical access and the threat of virus attack. Growing dependence on intelligent workstations and the legal liability issues related to storage of confidential data on microcomputers demand administration's attention.

Finally, business continuity/disaster recovery planning is gaining importance both in the business and academic community as dependence on computer systems continues to grow in nearly all fields.

[5]See Robert F. Curran, "Student Privacy in the Electronic Era: Legal Perspectives," *CAUSE/EFFECT*, Winter 1989, pp. 14-18.

Findings and Observations

Our findings can be related in the five identified areas.

Confidentiality

Confidential data are usually associated with administrative computing. Student records (demographics, grades, and personal and family financial information), grant and donor information, and a private institution's financial information are examples of confidential data. We found that:

- Financial information at public institutions is a matter of public record and is considered less confidential than at private institutions.

- The surveyed colleges and universities expressed concern about negative publicity regarding security breaches (computer virus, unauthorized disclosure of information and the like), believing that such publicity could affect funding efforts.

- All the surveyed institutions were aware of issues related to the confidentiality of data and had security measures that they believe to be appropriate in their circumstances.

- Participants did not believe that their existing confidentiality security measures would be changed substantially in the near future.

Telecommunications

Colleges and universities use telecommunications technology to: (1) support networks for administrative computing which involves distributed processing and remote data access; (2) support academic computing networks for research and instruction; and (3) provide delivery of information services to the public.

We found that survey participants are concerned about:

- Disruptions to computer processing due to damaged telecommunications
- The role of telecommunications in the spread of viruses
- Unauthorized access to computer processing via telecommunications
- Disclosure of confidential information via telecommunications

The surveyed institutions believed that a prolonged disruption to telecommunications could seriously hinder administrative and/or academic operations; however, they did not have disaster recovery plans in place that would ensure restoration of such capabilities within a reasonable time frame. Those we interviewed recognized that telecommunications technology is likely to give more users access to their institution's computing services, thereby increasing the risk of exposure to viruses and unauthorized access to confidential information.

Microcomputers

The most significant information security issues related to microcomputer use include viruses, local area networks which provide access to sensitive information, and legal concerns involving copyright violations.

We found that most of the surveyed institutions believe the information security threat associated with microcomputer use is limited because microcomputers typically are operated on a stand-alone basis (i.e., they are not connected to a network). According to the study participants, viruses had infected primarily free-standing personal computers.

Most survey participants considered their administrative computing systems to be relatively secure from viruses that lead to information security risks, which they associated more with academic computing. A virus in academic computers could interrupt all of an institution's academic computing. We found that cleaning up viruses is now considered a daily maintenance procedure.

Business Continuity/Disaster Recovery Planning

Most of the survey participants who indicated disaster recovery plans did not believe that they provide for the resumption of computing operations within a reasonable time after a major disruption in processing. Several participants indicated that executive administration at their institutions did not consider additional disaster recovery provisions to be warranted. All of the surveyed institutions were employing backup procedures and had off-site storage facilities.

Physical Security

Physical security issues—including loss of hardware and software due to theft or damage, and security breaches due to unauthorized use—were not major concerns of participants. Most surveyed institutions believed that their current physical security measures were adequately protecting hardware and software.

Effect of Security Breaches on Information Security Procedures and Controls

Participants discussed publicized incidents of security breaches and viruses, and how those incidents have changed their computer processing (mainframe, minicomputer, or microcomputer) procedures and controls. Notable findings in this area included:

- Publicized incidents of security breaches at other institutions have heightened information security awareness at most of the surveyed institutions. After such publicity, administration reviewed controls and procedures, and often concluded that security procedures at their institution were adequate.

- None of the surveyed institutions reported security breaches other than a virus infection.

- After a virus invaded their computers, four of the eight institutions changed their security controls and procedures. These changes included limiting the use of student-owned software, testing all software before execution, discouraging sharing of diskettes, reinforcing backup procedures, and instituting policy changes in the schools' bylaws.

Further Research

Use of telecommunications and computer technology in higher education is expanding and changing at a rapid rate. Additional research in this area would be valuable to ascertain:

- What priority do institutions of higher education assign the issues affecting information security?

- Are the priorities based on awareness, cost, or arbitrary decision-making?

- Are the priorities appropriate?

- Do institutions of higher education require the same degree of business continuity/disaster recovery planning as for-profit organizations?

- Is a major disruption to computing services a greater threat than is recognized by the surveyed institutions?

- Is the cost of developing and maintaining a disaster recovery plan warranted in the higher education environment?

Finally, further expansion of computer and telecommunications technology may increase the threat of computer viruses. Have institutions of higher education developed the policies and security procedures necessary to reduce the risk of spreading a computer virus across a network?

3—Risk Assessment

A risk assessment analyzes the existence and adequacy of computer controls that ensure:

- Confidentiality—sensitive data are identified and treated in a confidential manner.

- Integrity—data are kept complete, secure, and updated.

- Availability—data are accessible only to authorized users, and business continuity procedures are in effect for restoration of processing after a major interruption of computer processing.

Findings and Observations

Participants in our study were asked if their institution had conducted an objective security risk assessment within the last two years. While no overall risk assessments had been conducted, reviews of select areas of security had been performed (see Exhibit 3). Five participants indicated security procedures in sensitive areas were reviewed periodically by internal and external auditors.

Since the administration at most of the surveyed institutions had assessed specific areas of computer operations risks, they did not believe an overall risk assessment to be warranted; several participants, how-

ever, believed their institutions should establish a business continuity plan. One surveyed institution was in the process of conducting a security risk assessment for its administrative computing environment, including a review of their multi-campus telecommunications operations and the development of a disaster recovery plan.

Another institution in our study group had conducted a partial risk assessment. The resultant recommendations were described by information systems management as too general and not useful in enhancing the security and controls environment. Their experience illustrates the importance of defining the goals of a risk assessment before conducting the assessment to help ensure useful results. Furthermore, the assessment should include a cost/benefit analysis in support of the assessment recommendations. Without cost analysis, administrators may find it difficult to accurately determine the best course of action, resulting in a situation where needed security measures are not implemented.

Security measures can lose effectiveness over time. For example, password secrecy is frequently lost over time and the likelihood that encryption routines can be decoded increases with age. Risk needs to be regularly reassessed since all changes to a computer environment may affect previous conclusions and assessments.

As stated, most of the institutions in our study had not conducted a formal, objective risk assessment in at least two years. We found the risk management function at these institutions to be concerned primarily with insurance matters and protection of physical assets rather than with managing the risks associated with information security or business continuity.

Given the rapid change of computer and network technology, constant vigilance by those charged with protecting critical information assets is necessary. This should involve both daily scrutiny as well as periodic evaluations of the security measures in place.

Further Research

An objective risk assessment can put information security risks in perspective, and position executive administration to take a proactive stance. Further research could determine whether the climate exists in higher education for risk assessment. Is the need perceived? Are the full benefits of risk assessment known at the proper levels of administration?

Managing the information security risks associated with an institution's computing environment is as important as knowing what the risks are. Research in this area could disclose:

- How widespread is the risk management function in higher education?
- Does every institution need a risk management function?
- How extensive does a risk management function in higher education need to be?
- Should a security administrator function include the risk management duties associated with information security, or should institutions expand an existing risk management function?

Exhibit 3
Risk Assessment Reviews Conducted

	Number of Institutions Reporting
Performed overall risk assessment in last two years	0
Security risk assessed in specific areas within the last two years	4
Physical security	3
Division of duties	1
Disaster recovery plan	1
Reporting structure	1
Security policy	1
Security procedures	1

4—Information Security Policies

A security policy has at least the following four characteristics: (1) security guidelines for all operating environments (mainframe, minicomputer, microcomputer, local area network, and telecommunications), which encompass both administrative and academic computing; (2) personnel or a method for implementing, monitoring, and enforcing the policy; (3) methods for reviewing and amending the policy; and (4) methods of policy distribution.

The development and timely maintenance of a comprehensive and effective security policy is a challenging task. It is especially difficult if the responsibility for developing and implementing a policy is ill defined.

General Findings and Observations

A majority of the institutions surveyed did not have a stand-alone security policy. Exceptions were those that had a formal security administration function. The others were relying on codes of conduct and bylaws to establish guidelines on information security rules and conduct. Federal and state laws were also considered applicable to extreme cases, such as vandalism or theft. All institutions reported limited non-disclosure policies for student biographical and research data.

Fewer than half of the institutions in our study considered their policies current and adequate. Most surveyed institutions changed policies as required by law, but not necessarily in response to changing technology. One MIS director pointed out that the *existence* of security policies does not necessarily create awareness or guarantee enforcement.

We found that while none of the surveyed institutions had a security policy that included all of the characteristics described above, three institutions reported having security policies which meet most of the above characteristics, with the exception that the policies do not cover all computing activities or operating environments. One institution was in the process of developing a policy.

Some institutions without a separate security policy reported that their institutions' bylaws include general guidelines for using computer facilities, but they do not specifically address information security issues. Participants cited student brochures, departmental operations manuals, and the MIS organization monitoring for violations as additional methods for communicating and administering security procedures.

Enforcement is a sensitive issue in security administration at colleges and universities. The concept of academic freedom includes a degree of tolerance for experimentation and intellectual adventure, which may hinder the goals of security administrators. We found that the penalties for information security misconduct were often not defined, vaguely stated, or surprisingly lenient relative to those in non-campus settings. Though a change in this attitude is not necessarily called for, it is important to consider the possible implications of such an attitude.

Participants discussed the policies and tools they believe should be developed at their institution. Two of the three institutions that had security policies indicated that compliance to their policies could be enhanced by emphasizing awareness rather than punishment, and that the policies themselves could be enhanced by broadening them to include all computing environments. Among the institutions that had not developed a security policy, two believed that such a policy should be developed.

Findings and Observations about Microcomputer Policies

Our interviews gathered information about microcomputer policies and procedures at each institution. Exhibit 4 shows the quantitative results from this section of the study.

Of the institutions with a security policy, only one addressed microcomputer security specifically, and none addressed the use of microcomputers for sending and receiving executable programs. Some participants stated that their institutions' bylaws establish microcomputer security guidelines regarding such sensitive areas as copyright infringement, access procedures, and sharing diskettes.

Several participants reported difficulty enforcing microcomputer policies, with enforcement inconsistent and often depending on students policing themselves. Most participants reported penalties for violations are usually established on a case-by-case basis, primarily for violations of educational ethics, vandalism, or theft.

Exhibit 4
Microcomputer Security Policies and Procedures

	Number of Institutions Reporting
POLICY	
Specific microcomputer security policy	1
Reliance on code of conduct or bylaws for microcomputer security policies	5
Code of conduct/bylaws is adequate	2
ENFORCEMENT	
Department head	1
Computer lab monitors	1
Not assigned/not reportable	6
PENALTIES FOR INFRACTIONS	
No established procedures	5
Suspension	1
Revocation of password/access	2
Failing grades	1
Set by state laws	2
Student government	2
SOFTWARE USE REGULATIONS	
Procedures that differentiate between school-owned and student-owned software	0
Procedures governing use of software on institution's hardware	1
Procedures governing connecting institution's hardware to public bulletin boards to download and execute software	0
Microcomputer security procedures are keeping pace with technology	3

None of the surveyed institutions reported policies governing the use of student-owned software on institution-owned microcomputers, but one institution had procedures in this area. We found that microcomputer policies do not usually include provisions for connection to, and downloading software from, electronic bulletin boards, or executing such programs on school-owned equipment.

Most participants in our study reported that physical security of micro hardware and legal liability issues concerning copyright infringement are major concerns. Such concerns are addressed through student orientation, verbal and posted warnings, copyright notices, computer classes, and the institution's bylaws.

Further Research

Policies are most effective when they are consistently established, maintained, communicated, and monitored. It is important that policies are updated periodically to include evolving technology, and issued in a timely manner. A consistent pattern for developing, communicating, and monitoring information security policies was not evident in the surveyed institutions.

Additional research could help to gain a perspective on the following:

- Should security policies address the use of microcomputers?
- What procedures are needed to address the nature (i.e., binary vs. text) of data transmission?
- What is the academic user's view of such procedures?
- Would such procedures limit or restrict academic activities?
- What are the risks of not establishing such policies?
- Are institutional bylaws the appropriate vehicle to communicate information security policies?

5—Security and Control

Participants were asked to rank the effectiveness on a scale of 1 (lowest) to 5 (highest) of various campus computer groups (see Exhibit 5) for addressing security and control as well as other data processing issues (see Exhibit 6). The groups included:

- MIS Steering Committee
- Strategic Planning Committee
- Internal Audit Department
- Internal EDP Audit Function
- Risk Assessment Committee
- User Group
- Quality Assurance Group

Active participation by administrators and other computer systems users can contribute significantly to the introduction and integration of security concerns during the planning process. Various forums for such participation are found at most colleges and universities. According to the participants in our study, the effectiveness of those forums depends on the organizational seniority of the membership.

Although that relationship is not surprising, the quality of input given by senior administrators is affected by the degree of representation from the information systems organization. Quality input is more than the distillation and packaging of technical information and analyses. It should help to yield politically appropriate and fruitful responses to security issues. For example, one surveyed MIS director saw the public furor surrounding the Internet attack as an opportunity, because it caused widespread interest in security issues.

There is a trend in data administration in which responsibility for the security of the data is assigned to the user. Data custodians are assuming visible and active roles in deciding what data to secure and the appropriate protective measures necessary to secure those data. The advantage of this approach is that oversight duties and expertise are disseminated and duties are segregated.

Exhibit 5
Institutions' Use of Guidance Groups

	Number of Institutions Reporting
Internal Audit Department	7
Internal EDP Audit Function	6
Strategic Planning Committee	6
MIS Steering Committee	6
User Groups	4
Quality Assurance Group	2
Risk Assessment Committee	1

Findings and Observations

Participants ranked as the most effective in addressing issues of security and control the following groups:

- Strategic Planning Committee
- MIS Steering Committee
- User Groups
- Internal EDP Audit Function

These groups were identified as usually being concerned with security and control for administrative computing. Cited as the factors which contributed most to a group's effectiveness were the administration level of group members, the group's budget, and the degree of group activity.

Participants were also interviewed about security and control procedures in use and/or under review to protect hardware, software, and data. All of the institutions in the study were using conventional physical access restriction methods and all but one used security software.

Some of the surveyed institutions reported using security software packages such as ACF2, RACF, and TOP SECRET. Generally, participants considered these packages as tools for monitoring and accountability, not for enforcement. Participants reported that security violations are recorded and researched (on a more or less timely basis). If infractions are judged severe by those responsible for reviewing security violation reports, appropriate disciplinary actions are pursued. Infractions were considered infrequent and not a serious threat.

6—Information Security Administration

As stated earlier, a human resources commitment to security administration indicates administrative priorities in relation to information security. As defined in our study, a security administrator is responsible for: (1) developing, coordinating, and monitoring overall security procedures and plans; (2) developing, designing, and implementing security standards, policies, and procedures; and (3) monitoring compliance to security policies on a regular basis. The issues discussed concerned institutional commitment, both philosophical and financial, to security administration.

Findings and Observations

The description of the security administrator's function at three of the surveyed institutions met the criteria just described, but only two institutions had positions dedicated to security administration (see Exhibit 7) and they concentrated their efforts on administrative computing. The other six institutions did not employ a full-time security administrator, but assigned security administration duties to an individual in addition to his/her other job responsibilities.The small institutions and those with limited budgets did not have a full-time security administrator.

Participants were interviewed about executive administration's role in information security. Most believed that security issue discussions with executive management usually result from a specific event, such as a computer virus, unauthorized access to data, computer theft, or the like. Participants described administrators as reactive, interested in security issues primarily after a serious violation. One MIS director described such behavior as "event driven." Exhibit 8 summarizes executive administration's role in information security.

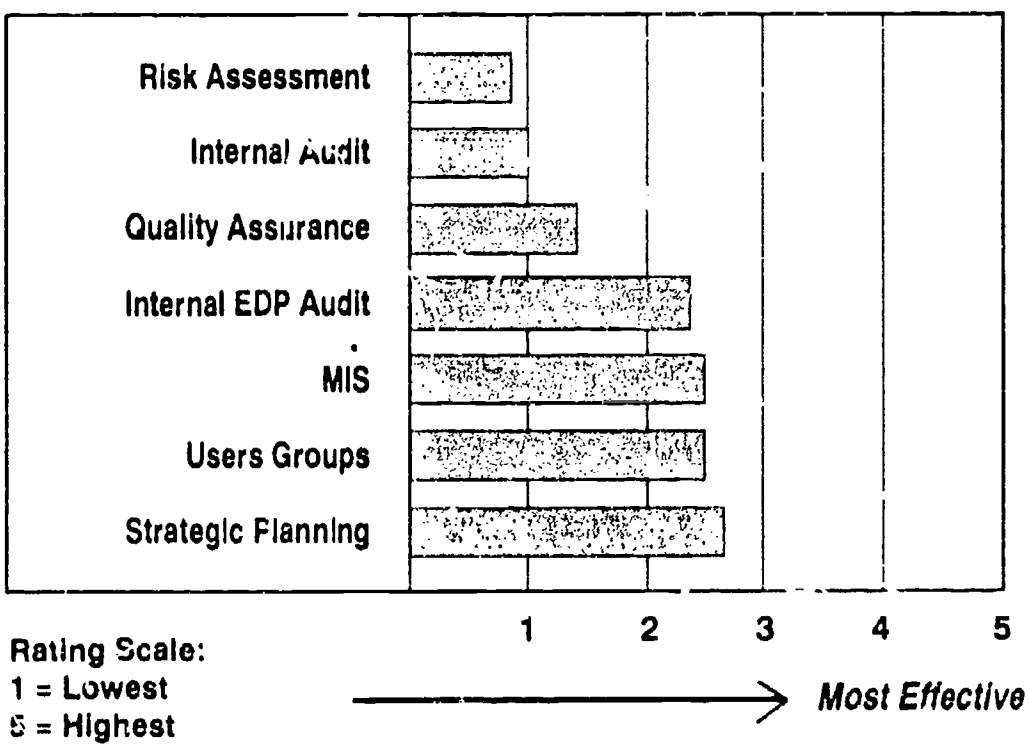
Most of the surveyed institutions expected no security budget increases or major enhancements to security policies in the next year.

Further Research

As changing technology places new demands on security systems, executive administration at institutions of higher education will need to make informed decisions and provide guidance on a broad range of information security issues. Further research in information security administration could answer:

- Does an institution's characteristics (i.e., size, funding, research orientation) correlate with the employment of a full-time security administrator?
- What are the risks associated with not employing a security administrator, given the rate of technological change?
- Should a security administrator also assume the role of network administrator?

Exhibit 6
Effectiveness Rating of Guidance Committees



7—Design, Review, and Testing of Information Security: The Role of Auditors and Consultants

Use of internal and external auditors is a resource available to information systems managers and administrators interested in addressing security concerns. Generally, auditors are perceived as after-the-fact reviewers of the information used to produce reports. Their technical expertise is viewed with skepticism; their involvement in the day-to-day affairs of the information technology organization is considered bothersome. In fact, they may give fresh insight in the analysis of security issues.[6] Internal auditors may have a broader view of the business needs of an institution than information systems staff. Similarly, external auditors may offer insight into how other institutions approach similar problems.

Findings and Observations

Participants were asked if auditors (internal or external) or consultants influenced the design, review, and testing of information security systems. They indicated their internal auditors generally play a minor role in the design, review, and testing of information security systems. Only one of the surveyed institutions reported using consultants to design, review, and test information security policies, methods, or procedures.

Overall, participants expressed a desire for greater participation by their internal auditors, and believed they could participate more effectively if they were provided with proper training in appropriate information security review and testing methodologies.

Participants at the surveyed institutions reported that as part of their audit procedures, external auditors usually review internal controls over the administrative computing activities, but not academic computing. Such reviews address security controls, but generally do not result in an in-depth analysis. Some participants indicated they would welcome comprehensive security reviews by external auditors.

Exhibit 7
Security Administrative Function

	Number of Institutions Reporting
Dedicated Security Administrator function	2
Security Administrator has other job function	6
RESPONSIBILITY DELEGATED TO	
IS Coordinator	1
Various MIS Staff	3
Systems Programmer	1
VP of Administration	1

Further Research

Successful institutions typically have internal auditors who can conduct EDP audits. In light of this, it would be interesting to know:

- What is the extent of EDP internal audit capability in higher education?
- Is the level of participation by EDP auditors in the design, review, and testing of information security systems appropriate?
- Do EDP internal auditors have the requisite skills to participate in the design, review, and testing of information security systems?

[6]See George Carroll, "Strengthening Security through Computer Center/EDP Auditing Teamwork," *CAUSE/EFFECT*, May 1986, p. 3, and Pamela Clem and Mark Olson, "Creating a Working Partnership with Your EDP Auditor," *CAUSE/EFFECT*, September 1987, pp. 14-18.

8—Information Security Issues for the 1990s

Two major developments will drive information security in the 1990s: the rapid growth of networks and network-based technologies (such as distributed databases) and the equally rapid growth of end-user computing on mainframes and microcomputers (spurred by the development and improvement of fourth-generation languages). Other value-added technologies, such as image processing, will create additional challenges for security administrators, such as access control of images. On the other hand, some new technologies may offer new tools to help security administrators, such as electronic signatures and biometric devices.

How best to provide for security will be the greatest challenge facing administrators, given the continuing trend toward dispersal and proliferation of critical data and access paths to critical data. Currently, it does not seem that information security is likely to keep pace with technological change. Security administrators will continually need to stay informed. Vendors can respond to market pressures to develop new security products, if they are made aware of how they can best help institutions meet their information security needs.

Findings and Observations

Participants cited the expanding use of networks and end-user computing, as well as the pace of technological advances, as the issues most likely to affect information security in the 1990s.

Networks

- There will be a substantial increase in use of inter- and intra-campus networks in administrative and academic computing.

- The increased number of users will increase the potential for unauthorized access to confidential data, particularly in situations where users have dial-up access. A major concern is how to secure confidential data and maintain network and data access control.

- Since networks will increase distributed processing and decentralized control, "data custodians" will play a major role in defining and controlling network security. Several of the participating institutions already use the data custodian concept by assigning the office(s) using the data the responsibility of security oversight.

- Several institutions suggested they will employ a network administrator to address the operational and security needs of the network.

- Other security issues related to distributed databases include wider use of distributed passwords, access across networks, and encryption and authentication across networks. Vendors may need to develop hardware and software to address those issues.

Exhibit 8
Executive Administration's Role in Information Security Administration

	Number of Institutions Reporting
Issues brought to executive administration's attention are typically event driven	7
SOURCE OF INFORMATION	
Internal Auditors	2
MIS/IS Director	7
The Press	4
External Auditors	1
MOST RECENT ISSUES DISCUSSED	
Physical security/theft	3
Virus	6
Unauthorized access	1
Employee vandalism	1
Data access issues	1
Hardware issues	1

End-User Computing

- End users may not know how to protect data, since end users are not under centralized control and are often untrained and inexperienced in data processing and computer use.

- Participants cited access control, maintaining confidentiality, and backup procedures as issues which needed to be addressed.

Pace of Technological Advances

Given the pace of advances in computer technology, participants discussed how they would meet the challenge of maintaining adequate security, identifying several technologies that are likely to affect their computer operations in this decade:

- Image processing will support storage of signatures, photographs, and documents for access and identity verification, student registration, transfer and storage of student applications and transcripts, and personnel records. However, image processing may raise significant concerns about access control and privacy, since the techniques necessary to secure image processing have not yet been fully developed.

- Paperless systems will be widely used in the future.

- Institutions will move away from transaction processing systems using written authorization, centrally controlled input and output, and printed transaction details. Systems for transferring transcripts, input and verification of grades, and processing financial aid applications are expected to allow for on-line authorization, recording, and processing with minimal manual intervention.

  Concerns include:
  — Providing access protection for electronic documents and signatures
  — Devising transaction control procedures
  — Improving quality assurance and testing methodologies during the development of such systems

- Some participants cited biometrics and artificial intelligence as potential authorization technologies. Most expected it will be years before institutions use such technologies.

Further Research

Additional research could seek answers to the following questions:

- As institutions of higher education adopt new technology and procedures (e.g., increased end-user computing, data custodians, and networking), will the information security requirements of new technologies require a foundation of information security built on today's technological base?

- Are institutions poised to adopt the new technologies and minimize any additional associated risks?

- Do institutions have the requisite experience to blend the security issues associated with the new technologies into their existing policies, procedures, and methodologies?

Concluding Observations

While the sophistication of technology continues to increase—allowing for faster, easier access to increased amounts of data and capability—the ability to adequately control access continues to lag. Our small study revealed several security and control issues which need to be addressed to reinforce the current framework. The ability to progress and keep pace in the 1990s will depend heavily on the framework of security and control methodologies developed today.

Colleges and universities will, in many ways, be in the forefront of these exciting developments. Their special need to be open and accessible while protecting critical or confidential information creates both challenges and opportunities. As is so often the case, striking the right balance between function and ease of use is difficult, especially where security issues are concerned. By their nature, institutions of higher education favor ease of use. However, their executive administration is faced with a complex combination of legal requirements and business needs for securing the privacy and integrity of sensitive information.

Scholars and students rigorously defend the rights they consider essential to academic freedom. Systems professionals, wary of the potentially negative consequences of "too much" openness, tend to lean toward greater security. Information technology executives in higher education must weigh all the conflicting factors and opinions and find the most suitable mix for their institution. Those who succeed will set new standards for their peers in corporate and government environments by finding ways to share resources productively and cost-effectively while protecting the critical data assets of their institutions.

Cost, as always, is an inescapable consideration. Effective security and control and meaningful contingency planning measures can be expensive. It may, however, prove more expensive in the long term to avoid the costs and assume attendant risks. The cost/benefit analysis is less bewildering once it is approached like a business decision. Security is simply part of the "cost of doing business."

So, the challenge is before us. All levels of personnel are challenged:

- Executive administration should maintain a high level of awareness of the issues affecting their environments and provide the resources necessary to address them.

- Information technology executives should continue to be cognizant of the security and control demands of the new technologies.

- Security administrators should disseminate awareness and information, spreading responsibility for security throughout their organizations.

- Users should elevate and maintain their level of awareness of their security and control responsibilities.

We trust our efforts at putting the issues and concerns of this important topic into perspective will be of assistance in meeting the challenges of the next decade and beyond.

Additional Reading

Balkan-Vickers, Lore. "Tailoring On-Line Access to Responsibility." *CAUSE/EFFECT,* November 1986, pp. 20-23, 27.

Berlind, David. "Viruses—Covert Invaders or Overrated?" *PC Week*, 27 November 1989.

Brown, Jana, and John O'Connell. "Distributed Use of a Fourth-Generation Language at Arizona State University." *CAUSE/EFFECT,* Winter 1989, pp. 25-29, 33-35.

Brown, Jean. "Establishing Policy Standards For Decentralized Electronic Information Management at the University of Delaware." *Records Management Quarterly,* April 1989.

Carroll, George A. "Strengthening Security Through Computer Center/EDP Auditing Teamwork." *CAUSE/EFFECT,* May 1986, p. 3.

Carson, Eugene W. "Distributed Access to Administrative Systems." *CAUSE/EFFECT,* September 1987, pp. 6-12.

Clem, Pamela, and Mark Olson. "Creating a Working Relationship With Your EDP Auditor." *CAUSE/EFFECT,* September 1987, pp. 14-18.

Curran, Robert F. "Student Privacy in the Electronic Era: Legal Perspectives." *CAUSE/EFFECT,* Winter 1989, pp. 14-18.

Denning, Peter J. *Computers Under Attack: Intruders, Worms, and Viruses.* Reading, Mass.: Addison-Wesley, 1990.

Hoffman, Lance J., ed. *Rogue Programs: Viruses, Worms, and Trojan Horses.* New York: Van Nostrand Reinhold, 1990.

Johnson, David R., Thomas P. Olson, and David G. Post. *A White Paper on Computer Viruses: Legal and Policy Issues Facing Colleges and Universities.* Washington, D.C.: ACE, 1989.

Kornel, Amiel. "Cramming for Educational Security." *Computerworld,* 6 November 1989.

Kung, M.T. "Software Security in the University Computer Laboratories." *Microcomputer,* May 1989.

Lonabocker, Louise. "Security In The Age of Distributed Processing," *College and University,* Spring 1990.

Lundell, Allan. *Virus! The Secret World of Computer Invaders that Breed and Destroy.* Chicago: Contemporary Books, 1989.

McAfee, John, and Colin Haynes. *Computer Viruses, Worms, Data Diddlers, Killer Programs and Other Threats to Your System: What They Are, How They Work, and How to Defend Your PC, Mac, or Mainframe.* New York: St. Martin's Press, 1989.

National Research Council System Security Study Committee. *Computers at Risk.* Washington, D.C.: National Academy Press, 1990.

Riggen, Gary. "Computer Security Systems Enable Access." *CAUSE/EFFECT,* Summer 1989, pp. 6-7, 48.

Ryland, Jane. "Security—A Sleeper Issue Comes into its Own." *CAUSE/EFFECT,* Winter 1989, pp. 8-13.

Staman, E. Michael. "Ownership, Privacy, Confidentiality, and Security of Data." *CAUSE/EFFECT,* July 1986, pp. 4-9.

Stoll, Clifford. *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage.* New York: Doubleday, 1989.

The Computer Worm, A Report to the Provost of Cornell University on an Investigation Conducted by the Commission of Preliminary Inquiry. Ithaca, N.Y.: Cornell University, 1989.

"The Cornell Commission On the Morris Worm," *Communications of the ACM,* June 1989.

Webster, Sally. "Ethics in the Information Age: After the Rules and Locks, What Do We Do?" *CAUSE/EFFECT,* Winter 1989, pp. 51-53.

IV

Appendix

Interview Guide Part I

1. What are the information security issues facing institutions today? Describe the institution's computing environment, e.g., administration, research, instructional, including organization/reporting responsibilities and security for each environment.

2. What are the information security issues that you face today in each described environment? Some issues to consider may be management, reliability, performance, and logical or physical access as related to:
   - Confidentiality—balance of security, accessibility, and productivity (academic freedom and security)
   - Threats—unauthorized access, viruses, interruption of IS services, theft of information, destruction of hardware/software
   - Microcomputers—LANs, stand-alone, on-line, up- and downloading, end-user computing, violations of software copyrights (software piracy)
   - Telecommunications—networking (WANs and MANs), dial-up, connectivity
   - Physical security—security and 24-hour availability by students (computer labs)
   - Business contingency planning and disaster recovery

   a. Administrative environment
      List and describe each issue. On a scale of 1-5 with 1 being the highest, rank each issue.

   b. Research environment
      List and describe each issue. On a scale of 1-5, with 1 being the highest, rank each issue.

   c. Instructional environment
      List and describe each issue. On a scale of 1-5, with 1 being the highest, rank each issue.

3. Do you consider information security awareness at this institution to be high, medium, low, or non-existent for each of the following:
   - Executive administration
   - Administration
   - Operational staff
   - Teachers
   - Students

4. Describe the methodologies used at this institution to maintain or reinforce information security awareness and specify the party responsible for each area. For example:

   - Incorporated into the employee and student orientation programs, system science courses, computer lab sessions; signs and procedures displayed in the computer center and computer lab building(s), etc.

- Physical security and monitoring procedures over access to information systems environment including microcomputer hardware and software for "labs" and administrative purposes.

5. Describe the institutional security policy as it relates to each computer environment.

   a. How often is it amended for changes to the environment?

   b. When was the last update?

   c. Does the policy address all the security issues discussed in question 2?

   d. Is the policy routinely communicated to all the computer departments?

   e. Describe how it is enforced.

6. As technology progresses, are the information systems security policies, techniques, and tools keeping pace?

7. What security policies and tools would you recommend be developed? Describe.

8. Is executive management routinely informed of information technology security issues?

   a. List the most recent issues brought to their attention.

   b. How were these issues communicated to them?
      - By you
      - The press
      - Internal auditors
      - External auditors
      - Other

9. Do you consider executive administration proactive or reactive to information security? Describe.

10. What percentage of information systems budget is allocated for security?

11. What commitment to information security has executive administration made in the last year? For example:

    - Development of or enhancements to information security policies; additional personnel, e.g., security administrator

    - Security software packages, e.g., RACF, ACF2, Top Secret

    - Increase in budget for security

12. Discuss the impact that an "information security problem," e.g., computer virus, unauthorized access to academic records, etc., would have on the institution. For example:

    - The institution could not attract top students: loss of research grants (both private and government), donations, and endowments; enrollment would decline due to poor public image; legal implications due to lawsuits, etc.

    - Recruiting and/or retaining staff.

Interview Guide Part II

What steps are being taken to address the information security concerns and issues?

NOTE: The information security issues and concerns from Part I are the basis for this section. Identify each issue and ensure it is addressed in this section.

1. Is there an established (formalized) security administration function?

   a. If so, describe the responsibilities, reporting structure, staff complement—part-time or full-time employee, staff assistant, professional security personnel, etc.—of this function.

   b. If not, why?
      - Not in the budget
      - Computer environment is too small

2. Are security and control methodologies either currently being employed or under review to protect assets in each computer environment, e.g., hardware, software, and information?

   Methodologies to consider include security software (RACF, ACF2, and TOP SECRET); access control devices, i.e., smart cards, proximity cards, swipe cards, key pads, security guard; contingency plan or disaster recovery plan.

   a. Does implementation adhere to policies?

3. Is computer activity monitored and are breaches of security investigated for each environment?

   a. Is monitoring on a 24-hour, 7-day-a-week basis?

   b. How are breaches of security that occur after "normal" business hours investigated?

   c. How are security violations dealt with? Are security privileges revoked?
      - If so, for how long?
      - If not, why?

4. Does the institution have the following:
   - Information systems steering committee
   - Strategic planning committee
   - Internal audit department
   - Internal EDP audit function
   - Risk assessment committee
   - User group participation in determining security policies
   - Quality assurance group
   - Other...

5. Describe the steps that are being taken to raise the security consciousness in each of the following groups at this institution.
   - Executive administration
   - Administration
   - Operational staff
   - Teachers
   - Students

a. Who is responsible?

b. Are the means effective? If not, why?

6. Has an objective assessment of security risk been performed within the last two years?

7. If so, did the results indicate that improvements should be made?

   a. Where appropriate, describe the nature of the recommended improvements as they may relate to:
      - Policy
      - Procedures
      - Operations
      - Physical access
      - Logical access

   b. What was executive administration's receptivity to the recommendations to improve information security?

   c. Is the implementation of the accepted recommendations proceeding on schedule? If not, why not?

   d. What recommendations were not approved for implementation? What were the reasons for not implementing the recommendations? For example:
      - Cost versus benefit was not acceptable
      - Funding was not in budget.

8. Have the incidences of computer viruses and breaches of security in colleges and universities resulted in changes to or increased focus upon information security in the various computer science courses at this institution?

   a. If so, please describe.

   b. If not, why?

   c. What is your opinion of the above?

9. Have the incidences of computer viruses and breaches of security in colleges and universities resulted in any changes to:
   - Mainframe software development procedures and controls?
   - Microcomputer usage procedures?

   a. If so, please describe.

   b. If not, why?

10. Are policies and procedures in place that set forth a code of conduct by which all student users of institutional microcomputers are expected to abide? If not, why not?

    a. Is the code of conduct adequate?

    b. What party is responsible for enforcing the code and how is enforcement carried out?

    c. How are infractions dealt with?

    d. If a code of conduct or statement of practices is in place:

- Does it differentiate between using the same software on a student-owned microcomputer vs. one owned by the institution?

- Does it properly address the policies and procedures by which software is allowed to be executed on the institution's microcomputers?

- Does it properly address the policies and procedures for utilizing the institution's microcomputers to connect to public bulletin boards and downloading software for execution in the institution's computer environments?

11. Do you consider the information security support that you are receiving from each of the following to be adequate?
    - Executive administration
    - Administration
    - Operational staff
    - Teachers
    - Students

    a. If so, why?

    b. If not, what additional resources would be required?

12. Describe the role that the institution's internal auditors, external auditors, or consultants have in design, review, and testing of information security.

    a. What methodologies do they employ to review and test security? For example:
        - Questionnaires
        - Independent audit used to analyze security software, i.e., RACF-DSMON, auditing through CICS, VTAM, SMF, etc.
        - Testing of network security, e.g., penetration studies

    b. How effective is each of their roles?

    c. Could the role of the internal auditors, external auditors, or consultants be expanded to improve the information security environment?

    d. Describe the role and prioritize the additional functions, services, software, or products that each group could provide.

Interview Guide Part III

What do you see as the information security issues of the institution in the 1990s?

NOTE: This section will generate a list of issues and possible solutions. The list should be prioritized using a scale of 1 to 5 (1 highest).

A partial list of concerns for the 1990s is:
- What impact will enhanced voice, data, and image transmission capabilities have on security?
- Will security advance at the same pace as technology?
- Proliferation of microcomputers, end-user computing, LANS, WANS, connectivity
- Costs of adequate information security
- Balancing of academic freedom, security, and technology needed to provide the best education in a competitive market, i.e., attract the best students; obtain grants, donations, and research funding; for public tax based institutions, public access to information
- Maintain a "proactive rather than a reactive" role in security environment

Coopers & Lybrand

Company Profile

Coopers & Lybrand is among the largest firms of professional consultants and accountants in the world. As part of an international partnership, the firm is represented in 100 nations and has a combined worldwide strength of over 44,000 partners and staff. In its 92-year history, Coopers & Lybrand has maintained its leadership position through its ability to anticipate and respond to the needs of its clients. The firm's industry-focused approach to the delivery of services is a key factor in its success.

Involvement in Higher Education

By any objective measure, Coopers & Lybrand is the nationally recognized advisor to higher education. The firm serves as the auditor and business advisor to many of the most prominent institutions of higher learning in America. Coopers & Lybrand audits hundreds of institutions including seven of the eight Ivy League schools and nine of the top ten private research universities. Coopers & Lybrand is also the acknowledged leader in higher education consulting, offering services clustered around six critical areas: Information Technology; Human Resources; Financial Management, Accounting, and Tax; Operations and Productivity; Facilities Management; and Governance, Organization, and Planning.

Range of Services

Information technology is the engine that directly supports the learning, research, and administrative functions of the institution. Rising costs, changing technology, and the increasing use and sophistication of software make the effective selection and use of computers a key management decision. Coopers & Lybrand has helped colleges and universities improve data and systems security, as well as design and successfully implement a wide variety of management information systems, and has worked with clients at every point in a systems life cycle. Information technology services include:

- Information Technology Audit and Security Services
- Technology Planning
- Decision Support Systems
- Application Readiness Assessments
- Computer Security
- Systems Planning and Implementation
- Database Development
- Networks and Communications
- Intellectual Property
- Chargeback/Cost Accounting
- Systems Integration

Coopers & Lybrand has assembled a team of experienced information technology consultants who work with colleges and universities on a full-time basis. The firm also has consultants who are specialists in enabling technologies such as:

- Database Management Systems (DBMS)
- Fourth-Generation Languages (4GLs)
- Expert Systems
- Voice, Data, and Image Networks
- Image Processing
- Electronic Data Interchange (EDI)

Recent Activity

These consultants bring a thorough understanding of the full systems development life cycle, including planning, requirements definition, design, development, testing, conversion, and implementation. The firm has reviewed and improved business processes and technology for registrars, bursars, financial aid directors, admissions officers, academic advisors, and alumni associations.

Listed below are some examples of how Coopers & Lybrand has helped its higher education clients improve their use of technology.

- Provided functional and technical assistance for the implementation of administrative packages
- Designed and built comprehensive endowment fund management systems
- Implemented financial decision support systems to improve budget management and planning
- Conducted numerous operations reviews of college information systems departments to help identify opportunities for improving information management
- Developed comprehensive administrative systems business models to help colleges and universities select and implement applications software
- Assessed the information technology organization and skills mix
- Provided information security risk assessment and control review

Coopers & Lybrand's consulting teams have broad experience in planning for and implementing complex administrative systems. The company's proven methodology for systems development and implementation (SUMMIT™) can be specifically tailored to meet its college and university clients' needs. Coopers & Lybrand offers its clients the right combination of higher education, technical, and project management skills needed to get the job done.

Coopers & Lybrand, a CAUSE member since 1983, has participated annually at the CAUSE national conference through vendor presentations and refreshment break sponsorships, and funded the publication of CAUSE Professional Paper #5, Information Security in Higher Education.

Contacts:

Clark L. Bernard
Joel W. Meyerson
John H. Duffy
Sean C. Rush
John Cassella
at
Coopers & Lybrand
One Post Office Square
Boston, Massachusetts 02109
(617) 574-5000

Albert Decker
Raymond Elliott
at
Coopers & Lybrand
1251 Avenue of the Americas
New York, New York 10020
(212) 536-2000

Professional Paper Series

#1 *A Single System Image: An Information Systems Strategy*
by Robert C. Heterick, Jr.

A discussion of the strategic planning for information systems, incorporating a description of the components needed to purvey an institution's information resources as though they were delivered from a single, integrated system. The "single system image," the vehicle through which tactical questions are resolved, comprises electronic mail, database access, print and plot service, and archival storage for all users. Funded by Digital Equipment Corporation. 22 pages. 1988. *$8 members, $16 non-members.*

#2 *Information Technology—Can It All Fit?*
Proceedings of the Current Issues Forum at the 1988 CAUSE National Conference

Based on the proceedings of the Current Issues Forum at the 1988 CAUSE National Conference in Nashville, Tennessee, where three panelists discussed information technology management on campus. Paige Mulhollan, Wright State University President, advocated a highly centralized management style; Robert Scott, Vice President for Finance at Harvard University, discussed the factors that led to a decentralized approach at Harvard; and Thomas W. West, Assistant Vice Chancellor for Computing and Communications Resources at The California State University System, explored alternative models for managing information resources. Funded by IBM Corporation. 17 pages. 1989. *$8 members, $16 non-members.*

#3 *An Information Technology Manager's Guide to Campus Phone Operations*
by Gene T. Sherron

A guide for managers of information technology faced with the challenge of integrating voice communications into the information technology infrastructure across campus. Taking a "primer" approach, this paper outlines the major issues in telecommunications facing campuses today, a quick look at the history of deregulation and effects of divestiture, a description of the basic components of the phone business—switch options, financing considerations, management systems, telephones, wiring, and ISDN—and a brief consideration of some of the management issues of a telecommunications organization. Funded by Northern Telecom. 26 pages. 1990. *$8 members, $16 non-members.*

#4 *The Chief Information Officer in Higher Education*
by James I. Penrod, Michael G. Dolence, and Judith V. Douglas

An overview of the chief information officer concept in higher education, including the results of a survey conducted by the authors in 1989. This paper examines the literature that has developed as increasing numbers of organizations in business, health care, and higher education have embraced the concept of managing information as a resource and addressed the need for a senior-level policy officer with responsibility for information technology throughout the enterprise. The authors provide an extensive literature review, including a discussion of industry surveys, and a bibliography of over 140 books and articles. Their survey results are included in the appendix. Funded by Deloitte & Touche. 42 pages. 1990. *$8 members, $16 non-members.*

#5 *Information Security in Higher Education*
by Raymond Elliott, Michael Young, Vincent Collins, David Frawley, and M. Lewis Temares

An examination of some of the key issues relating to information security on college and university campuses, based on in-depth interviews conducted by the authors at selected higher education institutions. Findings and observations are presented about information security awareness, policies, administration, control, issues and concerns, as well as risk assessment and the role of auditors and consultants in information security design, review, and testing. Funded by Coopers & Lybrand. 26 pages. 1991. *$8 members, $16 non-members.*

#6 *Open Access : A User Information System*
by Bernard W. Gleason

A discussion of the need to provide open access to all necessary campus information resources to administrators, faculty, and students. Based on his experiences at Boston College, the author offers design concepts and principles for a user information system providing open and easy access to information. In addition, the paper addresses many of the organizational, managerial, social, and political forces and issues that are consequences of an open access strategy on campus. Funded by Apple Computer, Inc. 24 pages. 1991. *$8 members, $16 non-members.*

You can order these publications via mail, fax, telephone, or e-mail:

CAUSE • 4840 Pearl East Circle, Suite 302E • Boulder, CO 80301
***Fax:* 303-440-0461 • *Phone:* 303-449-4430 • *E-mail:* orders@CAUSE.colorado.edu**

CAUSE is a nonprofit professional association whose mission is to promote effective planning, management, development, and evaluation of computing and information technologies in colleges and universities, and to help individual member representatives develop as professionals in the field of information technology management in higher education. Incorporated in 1971, the association serves its membership of more than 900 campuses and 2,500 individuals from the CAUSE national headquarters at Suite 302E, 4840 Pearl East Circle, Boulder, Colorado 80301. For further information phone (303) 449-4430 or send electronic mail to: info@CAUSE.colorado.edu.

CAUSE is an Equal Opportunity Employer and is dedicated to a policy that fosters mutual respect and equality for all persons. The association will take affirmative action to ensure that it does not discriminate on the basis of age, color, religion, creed, disability, marital status, veteran status, national origin, race, or sex, and actively encourages members and other participants in CAUSE-related activities to respect this policy.