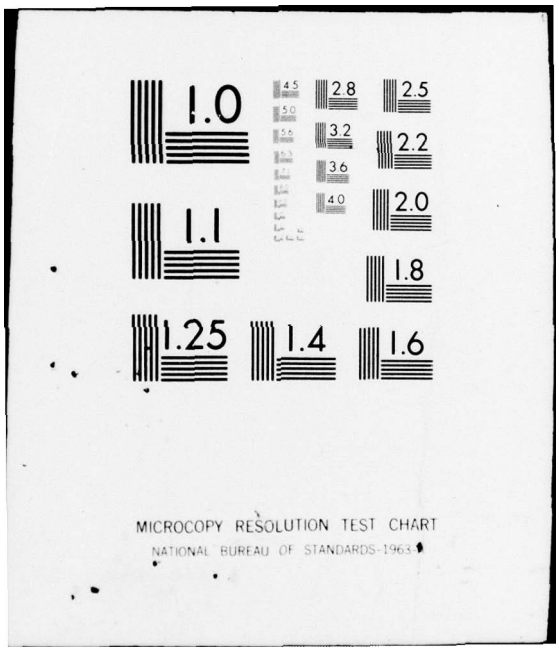
AD-A045 057 CALIFORNIA UNIV LOS ANGELES GRADUATE SCHOOL OF MANAGEMENT F/G 9/4
THE VULNERABILITY OF COMPUTER AUDITING.(U)
MAR 77 B P LIENTZ, I R WEISS
N00014-75-C-0266

UNCLASSIFIED TR-77-1 NL

| OF |
AD
A045057

END
DATE FILMED
11-77
DDC


1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
5.6
MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

Bennet P. Lientz, Ph.D., and Ira R. Weiss, Ph.D.

The Vulnerability of Computer Auditing*

Some of the problems associated with computer auditing are related to AICPA Statement on Auditing Standard No. 3. The authors propose means for dealing with the problems until improved internal computer security methods are implemented.

Bennet P. Lientz, Ph.D., Associate Professor of Computers and Information Systems, Graduate School of Management, University of California, L.A., is author of many papers and a textbook on information systems. Ira R. Weiss, Ph.D. (pictured above), Assistant Professor of Accounting and Information Systems, Graduate School of Business, NYU, is currently developing an in-depth computer auditing course for NYU.

Introduction

Most auditing procedures for computer-based systems relate only to those aspects that can be readily reviewed and understood. The problem, however, is much more general and includes the *total environment* of the system including operating systems and telecommunications. This environment has been shown to be vulnerable in such a way that it may affect the financial condition and life cycle of the firm. Examples of this vulnerability are cited in a report of Stanford Research Institute.[1] Even with the most sophisticated organizational and application controls, the remaining parts of the systems environment are substantial and the problems associated with these elements can be catastrophic to the organization.

From reviewing the AICPA Statement on Auditing Standards No. 3 (SAS No. 3) and some of the literature on computer auditing, it becomes evident that more is needed to insure the integrity of the systems being audited. Further auditing procedures must be instituted to insure compliance with the *intent* of SAS No. 3.

What Is SAS No. 3?

SAS No. 3 indicates that internal controls in the data processing installation should be evaluated when computers are used in processing a significant number of accounting applications. SAS No. 3 further points out that the auditing examination should be performed by persons with adequate technical training as auditors. In evaluating a computer-based system, this implies that auditors must not only be competent in understanding audit objectives, but also in understanding of computer concepts to be able to identify the strengths and weaknesses of the system.

SAS No. 3 points to several types of controls that should be evaluated, including the following:

1. Organizational plan and operation of activities;
2. Procedures relating to documentation, review, testing and approval of systems and systems changes;
3. Controls for hardware;
4. Access controls to equipment and files;
5. Application controls relating to input, processing and output;
6. Segregation of functions relating to both manual and computer operations (e.g., the same person should not be allowed to write a program to process vendor invoices and be able to submit transactions to that program for operational processing).

In concluding, the statement considers some procedures to review these controls.

Computer Auditing—State of the Art

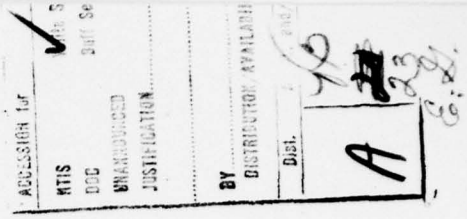
Today, over 100,000 computers are in use worldwide with over 80 percent of these storing and processing financial records.[2] In terms of SAS No. 3, a good portion of these installations are processing a significant amount of accounting information and should be evaluated, as part of the organization, for strengths and weaknesses in the control functions. Yet, many companies are doing today's computer audit work with yesterday's auditing expertise in terms of experience and education.[3] The EDP environment has changed substantially in the last decade. Unit record equip-

* This work was partially supported by the Information Systems Program, Office of Naval Research, under contract N000014-75-C-0266, project no. 049-345.

[1] Donald B. Parker, "Report to the 5th Conference on Computer Abuse," Stanford Research Institute, 1973.

[2] Robert L. Stone, "Who Is Responsible for Computer Fraud," *Journal of Accountancy*, February 1975.

[3] Joseph Wasserman, "Selecting a Computer Audit Package," *Journal of Accountancy*, April 1974.



ment techniques have evolved into sophisticated operating systems, teleprocessing, data base systems, multiprogramming and multiprocessing environments.[4] We would expect the firm which possesses these processing capabilities to have more technical expertise in an operational sense than an independent auditor, when the auditor has not been trained as a technical computer information systems specialist.

What is the impact of this progress on the auditor? The traditional internal control evaluation becomes somewhat more complex. Areas of concern are segregation of duties which might be blurred by highly integrative systems and the partial or total disappearance of the audit trail.[5] These developments give rise to a multiplicity of interactions within advanced systems, on a real-time basis, widening the potential error rate and potential fraudulent activity at any given time. After-the-fact tests of compliance and control may be insufficient to meet present day audit requirements.[6] The number of transactions processed daily, projected to a monthly basis, could be so voluminous that a center undergoing undetected penetration or errors in processing could be so severely affected that the going concern concept for that company could become invalid prior to an in-depth audit. Therefore, the need for *continuous* system integrity reviews appears imperative.

Again, what are the implications of these problems to the auditor? The auditor in the attest function states that the financial statements fairly represent the financial position of the company. Given an unqualified statement the auditor by implication states that the firm's liquidity is adequate to support the going concern concept. Yet there have been many cases of documented computer abuse totaling in the millions of dollars. After the fact auditing might in fact locate abuses, but there is still the issue of responsibility for loss if the firm cannot recover from these abuses. In Equity Funding management, auditors and computer vendors were all named as parties to a "computer" fraud.

What then is the current state of the art in computer auditing? Computer auditing may be considered as having two component parts. First, the computer is utilized in many audits as a *tool*. Extension testing, depreciation calculations, present values, footing, confirmations, aging, statistical sampling, etc. are some of the functions that can be accomplished through the computer on a timely and cost/effective basis. This aspect of computer auditing is being utilized with great frequency.[7] The auditor is able to identify direct benefits from this audit tool and the audit can then be a scientifically sampled verification of financial statements *rather than a heavy clerical burden.*

The second aspect of computer auditing can be referred to as *data center reviews*, which encompasses the main thrust of SAS No. 3. This entails a review and analysis of operations, security, applications and general internal control functional tests. Here the auditor is faced with some problems. Levine[8] depicts 11 basic concerns of the auditor in this area, highlighted by keeping current in EDP and its audit impact. He also addresses some aspects of what auditors need to enable them to address the audit with sufficient competency including utilization of monitoring systems, methods of evaluating systems' integrity and standard software controls. Weber[9] goes further by insisting that operating systems be audited periodically because the integrity of the entire system is controlled by the operating system. Yet, since the technical aspects of operating systems are so complex, the auditor views this aspect as a low risk area. This *may be a critical error of the auditor* and will be discussed further in the next section.

To summarize the state of the art, the auditor utilizes the computer as a *tool* in a relatively efficient manner. But in a *data center review* the extent to which controls are evaluated is often limited to the visible physical security and applications controls. In doing this the auditor relies on technical systems such as telecommunication networks and operating systems that in fact might be used to override and change the very applications that have been audited, judged appropriate and outputs relied on without extensive substantive testing.

Problems Remaining

As pointed out in the previous two sections, there are areas of the systems environment that are not explicity addressed by SAS No. 3. *For example, suppose a system is* operational within a computer mode and a penetrator is seeking to enter the system and gain access to data and/or programs by using a terminal. If the computer system is a general time-sharing system, the data and programs are available to authorized users during certain times. The data and programs could relate to accounts payable, inventory shipments, personnel data or product development.

The penetrator first attempts to enter the system using the telecommunications network. Even if the system is password protected, and the password cannot be broken, the penetrator can resort to masquerading (penetrator represents an authorized user), eavesdropping (listening in at random), wiretapping (listening at determined times and recording data over the lines), piggybacking or between lines (penetrator uses system when the authorized user is signed on but not active, or is given disguised messages). Alternatively, the penetrator may be able to deduce the authorized users' password by the characteristics of room location, initials, social security number, birthdate, address or other data obtainable pertaining to authorized users.

After the penetrator has successfully entered the system, an

---

[4] Editorial, "Technical Proficiency for Auditing Computer Processed Accounting Records," *Journal of Accountancy*, October 1975.

[5] Carl Pabst, "What's All the Fuss About EDP," *California CPA Quarterly*, June 1974.

[6] George Rittersbach and S. Harlan Jr., "Auditing Advanced Systems," *Journal of Accountancy*, June 1974.

[7] Everett C. Johnson, "The Computer As an Audit Tool," *California CPA Quarterly*.

[8] E. G. Levine, "Auditing Requirements for Advanced Systems," *Journal of Accountancy*, March 1974.

[9] Ron Weber, "An Audit Perspective of Operating System Security," *Journal of Accountancy*, September 1975.

attempt can be made to override the operating system and move into the privileged mode (where the penetrator has the ability to affect the system itself). At this point the penetrator disables or diverts the computer accounting system such that the activity (i.e., audit trail) of the system is blurred. Now the penetrator can initiate unauthorized transactions, alter program and systems logic, destroy information, obtain or view highly sensitive information or can accomplish all that is possible by his or her own creativity. The penetrator now having completed the above task signs off the computer system undetected.

There are several implications in this simple example. First, unauthorized transactions can seriously impair the operational integrity of the system. The financial statements, depending on the system, may not reflect the true state of affairs of the company. A second implication is the recognition that competition within an industry combined with precedents of lenient attitudes toward white collar crime and the available technology makes such approaches more attractive and limited in risk. A third implication is that if only the content of SAS No. 3 is followed, the internal controls could be judged sufficient, giving the auditor comfort in relying on the outputs generated, when in fact they were not due to the computer and communications environment of the system (i.e., possibility of penetration).

To summarize, these three implications may impact the firm which relies heavily on computer systems by indicating the threat, the effect on operations, financial statements and the on-going concern concept, and the need for additional and more sophisticated controls.

Security Measures

One study[10] has indicated that there are no secure operating systems commercially available and that there is no way today of certifying secure computer systems. It is essential then that interim measures be employed until secure operating systems become a reality.[11]

Exhibit I represents a table of penetration methods, recovery measures if penetrated, preventive security measures and cost elements of implementing the security measures. This Exhibit can be utilized to address the example presented earlier. To counteract penetration of communication lines: data can be encrypted (coded), system-generated random dialogues utilized (system queries user at random with regard to personal characteristics), alternate routing of messages and multiple passwords per transaction can be required. The techniques in the computer center itself include encrypted files and programs, automatic cancellations upon unauthorized attempted access, accounting programs that are not controlled by operating systems, but by input/output controllers, disk controllers that are hardwired for security techniques and access authorization.

The Exhibit is not all inclusive, but represents some techniques that can be employed when weaknesses are discovered in the operations of a data center. The auditor should be aware that there are interim techniques available to partially control access and penetration when these are considered high-risk areas.

In general, there should always be passwords on files when possible, read/write restrictions if appropriate, accounting systems, programs in load module form and counteractive systems measures when mistakes are made either in the log-on procedure or access procedure. Starting with the above measures, utilizing some methods given in the table and employing intelligent and alert personnel will insure more confidence and less risk within the computer system.

Developing Cost-Effective Approaches to Security

Implementing all possible countermeasures is not warranted or cost effective. Overkill to counteract improbable penetration can severely affect the cost and performance of systems. Organizations and independent auditors can employ simulation techniques and risk analysis[12] to identify the highly sensitive and exposed areas where the major control efforts should be placed.

There are basically three areas to be observed when reviewing the internal controls of data centers: operations, physical security and software security. For operations, the same guidelines should be imposed as when reviewing manual systems. Typical functional areas are: input, operations, programming and maintenance, library and output. When the organizational framework is set-up in this manner, the review can be structured to look at segregation of duties and control functions. The librarian controls programs and data while the input section controls new transactions. The programming and maintenance functions are separate. Therefore, there is no possibility of changing programs to fit new data. Controls that can be implemented are logging procedures of programs utilized, authorization for programming changes, appropriate dissemination of output and explicit operational directions for operators. A wealth of literature is available describing adequate physical security.[13]

The approach to reviewing software security is not defined as precisely as the other areas. One reason for this is that, given the most sophisticated software security available, penetration may still be possible. The approach must be a probability technique accessing high risk areas. Once these areas have been identified, one can pick the measure available that would most satisfy, in cost and performance, that particular need.

The most effective approach might be the one most common to auditors today, the questionnaire. Through this method we try to quantify both the impact and proba-

---

[10] IBM, "Data Security and Data Processing," IBM Corporation, G320-1370-0, 1974.

[11] R. C. Canning, "Protecting Valuable Data: Part II," *EDP Analyzer*, February 1974.

[12] J. J. Martin, *Security Accuracy and Privacy in Computer Systems*, Englewood Cliffs, N. J.: Prentice-Hall, 1973.

[13] "The Considerations of Physical Security in a Computer Environment," IBM Corporation Manual, C520-2700, 1972.

EXHIBIT I
Event List

Event	Recovery Measure	Preventive Measure	Elements of Cost
Attempts through communication lines (see definitions under "Problems Remaining")			
• Masquerading	Retain back-up files	Levels of Passwords Transformation Functions Random Dialogues Encrypted Files	Software costs Encryption/Decryption Devices (coding and decoding) Effect on System Performance—increased systems overhead
• Wiretapping/Eavesdropping	Retain back-up files	Cryptography Alternate Routing of Messages	Softward Costs Encryption/Decryption Devices Effect on System Performance
• Piggybacking or Between Lines	Retain back-up files	Cryptography Random Dialogues Levels of Passwords Continuous Passwords With Each Transaction Automatic Shut Offs After *n* Seconds of Nonuse	Software Costs Encryption/Decryption Devices Effect on System Performance
Attempts through Computer Systems			
• Unauthorized Attempt to Enter System	Retain back-up files	All Identification/Authorization Measures (a) passwords (b) dialogues (c) transformation functions (d) magnetically encoded cards If detected immediate disabling actions	Software Costs Effect on System Performance
• Browsing	Retain back-up files/ none	Functional Passwords Transformations Read/Write Restrict Encrypted Files Intelligent Disk Controllers	Software Costs Hardware Costs Encryption/Decryption Devices Effect on System Performance
• Override Operating System	Retain back-up files/ none	Automatic Cancellations Upon Unauthorized Action Accounting System Independent of Operating System System Monitors Encrypted Files	Software Costs Personnel Costs Encryption/Decryption Devices Effect on System Performance

bility of an occurrence. This enables the following questions to be addressed. Can the occurrence be tolerated? Can the dollar impact be lowered or can the probability be lessened? This type of analysis measures the value of an asset to the firm and the amount of resources to allocate to the asset for protection. For example, a system might contain two resident disk packs. On one, pack data pertaining to census information is stored. On the other, product development information is stored. Each disk has an equal probability of being penetrated. Yet the outcomes of successful penetration are quite different depending on which pack is chosen. We can tolerate penetration of the census data. It is public information and at worst duplication would be the final outcome for the firm. It is obvious that the answer dramatically changes under the product development assumption. Here penetration cannot be tolerated, so that there is concern about the dollar impact and about lessening the probability of penetration. We have now put a new type of value on an asset. We might call it an *exposure value* or *cost of loss* of exclusive use. Though product development information may be totally useless without proper demographics, the information, considering exposure value, is quite different.

Through Exhibit 2 we attempt to give the organization and independent auditor some points to consider and questions to answer to develop proper exposure values or probabilities of penetration. There is no clear-cut method of achieving these values since they are installation dependent. As the exposure of an asset widens through its uninterrupted accessibility, the risk of exposure is in-

EXHIBIT 2
Risk Analysis Questionnaire

Telecommunications
- Identify systems that are dependent on telecommunications
- What are the log-on procedures?
  - Do they remain constant or change?
- What type of data is transmitted?
- What is the sensitivity of the data?
- What is the frequency of data transmission?
- What is the volume of data transmission?
- What has been the experience with retransmission or lost messages?
- Are telecommunication systems data entry systems only or retrieval and processing systems as well?
- Is the system restricted to certain terminals or can the system be dialed up from any compatible terminal?
- What type of communication system?
- Are long time lags experienced between responses?
- Are the users of the system heterogeneous or homogeneous organizationally?
- What security procedures are currently employed?

Computer Operations
- Identify on-line systems
- What are the log-on procedures?
  - Do they remain constant or change?
- Are all programs/data protected in some manner?
  - Password protection?
  - Encryption?
  - Read/Write restrictions?
  - Do they remain constant or change?
- Does the operating system control the checking procedures for the protection methods?
- Has, to your knowledge, the operating system, either intentionally or accidently, been overridden?
- Have requests been made to your system which were answered by data irrelevant to the question, but considered sensitive data?
- Is there an up-to-date accounting program employed by your system?
  - Is it controlled by the operating system?
- Are there procedures employed to cancel programs that exceed their authority?
- Are all vendor supplied security features employed?
  - If not, why not?
- Are there periodic checks that current production programs conform to the authorized version?
- Can a program be run if it is not cataloged?
- Organizationally speaking, is the computer used by a heterogeneous or homogeneous set of people?
- What are the security features currently employed?

creased. It is then up to installation management or independent auditors to consider whether resources should be allocated to that asset.

This approach can serve as a guideline for the design and the continuous auditing of the system. The approach aims to identify where controls should be placed to assure reasonable processing of data in a cost effective manner.

Conclusion

With the development of SAS No. 3, the independent auditing firm that audits clients with significant accounting computer-based applications systems has more responsibility for assessing computer-based controls. The responsibility must be met with technical expertise and an understanding of the environment of application systems for computers and telecommunications. The scope of controls necessitated by this environment must be broadened and the auditing firm must be knowledgeable enough to audit the total system to address these elements of the environment.Ω

Indenture's History

The modern finance term "indenture," referring to the legal agreement between the corporation issuing the bonds and the trustee representing the bondholders covering terms of the bond issue and the restrictions placed on the company, had its origin in colonial America. Individuals wishing to come to America would bind themselves to a master in America in return for their passage over. In this system of temporary servitude, upon the completion of a period of service, the individual would earn his freedom. These people were known as "indentured" servants "because of the papers recording the contract, papers which were cut or torn with an indentured edge so that the two copies, one going to the master and the other to the servant, would correspond." – Excerpt from "200 Years Ago in Accounting," by Lawrence C. Sundby, Ph.D. and Robert C. Kehm, CPA. *The People of Arthur Andersen & Co.*, September 1976.

Unclassified

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER (14) TR-77-1 Technical Report

2. GOVT ACCESSION NO. (9)

3. RECIPIENT'S CATALOG NUMBER — Technical rept.

4. TITLE (and Subtitle) (6)

The Vulnerability of Computer Auditing

5. TYPE OF REPORT & PERIOD COVERED

6. PERFORMING ORG. REPORT NUMBER

7. AUTHOR(s) (10)

Bennet P. Lientz and Ira R. Weiss

8. CONTRACT OR GRANT NUMBER(s) (15)

N00014-75-C-0266

9. PERFORMING ORGANIZATION NAME AND ADDRESS

Graduate School of Management
University of California, Los Angeles 90024

10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS

NR 049-345

11. CONTROLLING OFFICE NAME AND ADDRESS (11)

Information Systems Program
Office of Naval Research, Arlington, Va.

12. REPORT DATE

March 1977

13. NUMBER OF PAGES

5

14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)

----- (12) 6p.

15. SECURITY CLASS. (of this report)

unclassified

15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

distribution of this documnnt is unlimited

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

-----

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Computer auditing
Security measures
Software controls

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

An analysis is made of potential security methods that can be employed until there exists more secure systems. Cost-effectiveness of security measures is examined along with recovery and preventive measures. Risk analysis questions are raised.

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE
S/N 0102-014-6601

unclassified
SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)