UCRL-13573

MANUAL FOR INVESTIGATION OF COMPUTER-RELATED INCIDENTS OF INTENTIONALLY CAUSED LOSSES, INJURIES, AND DAMAGE

Donn B. Parker, Stanford Research Institute

February 1973

Prepared under subcontract to:

The RISOS Project
Lawrence Livermore Laboratory
Contract No. AT(04-3)-115

Prepared for U.S. Atomic Energy Commission under contract No. W-7405-Eng-48

LAWRENCE LIVERMORE LABORATORY

University of California/Livermore

The RISOS Project is sponsored by the Advanced Research Projects Agency of the Department of Defense under ARPA Order No. 2166.

LAWRENCE LIVERMORE LABORATORY
University of California · Livermore, California · 94550

UCRL-13573

MANUAL FOR INVESTIGATION OF COMPUTER-RELATED INCIDENTS OF INTENTIONALLY CAUSED LOSSES, INJURIES, AND DAMAGE

Donn B. Parker, Stanford Research Institute

MS. date: February 1973

NOTICE

This report was prepared as an account of work sponsored by the United States Government. Neither the United States nor the United States Atomic Energy Commission, nor any of their employees, nor any of their contractors, subcontractors, or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness or usefulness of any information, apparatus, product or process disclosed, or represents that its use would not infringe privately owned rights.

CONTENTS

ILLUSTRATION

Introduction

Unauthorized acts involving computer systems result or could result in losses, damages, or injuries and are occurring with increasing frequency and seriousness. This is caused by the increasing numbers of computers, the proliferation of computer applications in vital and sensitive activities of society, and the lagging means and resources applied to protection. Unauthorized acts range from criminal acts as defined by criminal law to civil disputes, acts resulting in private sanctions, and disputes between people or organizations.

These acts involve computers in three ways:

- A computer can be the subject of the act such as in vandalism causing hardware damage, software failures, or media (data and their containers) losses.
- A computer can represent a unique environment in which an act can occur--such as the theft of a computer program.
- A computer can be used as a tool in the perpetration of an act where the act and its results may not be associated with computer processing.

It is important to investigate and study real incidents. We gain insight for developing the methods to deter, prevent, detect, and recover from incidents resulting in losses, injuries, and damages; and we justify the expenditure of appropriate amounts of resources. This empirical approach of studying real cases is as important as the theoretical and conceptual approaches to solving the problem. Whether the acts studied are intentional or accidental is of less interest than the ways that they occurred; however, intentional acts represent more of a challenge to detect and prevent, and protection from them also is protection from accidental acts. It is important to limit investigations only to incidents where new insights may be gained. However, it is important to record all incidents to determine frequency and occurrence.

Four levels of activity are suggested:

- Record all discovered incidents
- Analyze each incident to determine if further investigation is warranted
- Investigate in detail and document selected cases
- Aggregate findings to support theories and approaches to problem solution.

A computer-related incident investigation questionnaire has been designed to document detailed investigations in a standard form and to facilitate aggregation of findings. The questionnaire is, however, too detailed and highly structured to be filled out during the investigation. Rather, it should be used as a guide to ensure completeness of investigations; it should be filled out from field notes and recollection following investigations. It consists mostly of objective questions with multiple choice answers as an aid to aggregate information over all cases investigated and to facilitate standardization of terminology. Sections for subjective, narrative descriptions are also provided where appropriate. Key word extraction and space for coding the narrative content provide means for extracting objective, standardized information even for these sections. (See Appendix A.)

Sources of Incident Reportings and Information

Source Reliability

One of the important purposes of incident investigations is to separate fact from fiction to avoid wasting security resources to protect against fictitious or distorted threats. For example, even in reputable publications such as the Harvard Business Review or technical conference proceedings, otherwise respected authors frequently report incidents that have no basis in fact, are untrue, distorted, or irrelevant to computers. The use of newspaper clipping services will result in a deluge of irrelevant information especially about computer errors unless well-trained people are employed to separate the different categories of information. Newspaper articles are usually inaccurate and distorted and should not be relied on except as indicators that something of interest may have happened. Incidents documented only from the public media should always be classified as unverified. Personal, direct contact with a reliable source such as a participant in or witness to the incident is required to classify a case as verified.

Locating Sources

Finding sources of information includes finding people and documents. Always start with the telephone and write letters when there is time. People can be located from information in newspaper articles, from police, and from court records. Telephone information operators are surprisingly helpful in locating people and organizations. Standard library reference books help in locating organizations. Ask secretaries, telephone operators, librarians, and clerks for more information than you expect them to have.

One kind of source comes from having governmental authority where laws, regulations, or judicial authority force the reporting of incidents to an investigatory agency. Another kind functions without this authority;

the sources are voluntary, are publicly revealed usually through newspapers, or involve legal actions resulting in public documents. Investigations without authority are assumed to be the type this manual treats; thus, investigations with authority become a special case. Investigation with authority is amenable to the same kind of methodology described here. Newspapers, trade papers and journals, police arrest records, and court records provide the most comprehensive sources. Publicity of the investigative activities and extensive communication with information sources in business, government, and trade and professional associations can produce voluntarily reported incidents. However, most organizations will deny that they have been the victims of confidentially handled incidents and even of some publicly reported incidents. Victims often will play down any role the computer may have played because of their continued high level of vulnerability through their Electronic Data Processing (EDP) activities. Nevertheless, they will often reveal information about incidents where other organizations, especially competitors, have been victims. Banks are particularly sensitive victims in trying to maintain their fiduciary responsibilities.

Documents other than from the public media include press releases that provide more accurate details and legal documents. It is better to get copies of legal documents from prosecutors, lawyers, or victims when possible. They can also be obtained from the clerks of the courts that have jurisdiction, but they often cost up to $0.75 per page. Normally, court documents can be studied in the court clerk's office. Legal documents include:

- Police crime reports
- Criminal and civil complaints
- Police continuation reports
- Answers of defendants

- Search warrants
- Arrest warrants
- Court orders and injunctions
- Affidavits
- Depositions or declarations
- Court reporter trial transcripts
- Memorandums of decisions, verdicts, sentences, and appeals
- Trial memcranda
- Appellate briefs and decisions.

People who may be reliable sources of information cover a wide range of roles in an incident. They are listed below in generally the declining order of importance, based on actual investigation experience. Helpful comments and possible means of contact are also supplied were appropriate.

- Other investigators who have EDP background and are familiar with the case. Start with what has already been learned.
- Police officers, including detectives and district attorneys' investigators, are usually eager to cooperate if they are assured of receiving credit for being the source of the information. This is because they attempt to advance themselves in their jobs by gaining exposure in highly publicized cases; however, they tend to be inaccurate on technical subjects involving computers and often do not understand the real substance of a case.
- Other investigators including news and magazine reporters and writers, but the above warnings about reliable sources apply.
- Suspects and known perpetrators are usually willing or eager to talk to objective investigators about their acts if unconstrained by pending legal proceedings. Their stories, however, are usually strongly rationalized to justify their actions. They probably put as much effort into rationalizing their acts as in perpetrating them. Information from suspects must be strongly balanced with information from the other sources. A case report is usually of less value if the suspect's story has not been documented. Suspects are

usually easy to find unless they are trying to avoid publicity. If criminal charges are involved, they can be found at their preliminary hearings. Their lawyers are often a source of contact. It must be remembered that the suspects and perpetrators are the threats on which prevention resources are being spent.

- Witnesses with EDP background may have witnessed the planning or at least part of the actions or the results of the incident. They may be reluctant to talk for fear of incriminating themselves or being identified with the case. They may be protecting a victim or suspect. It is important to ask all other participants for names of witnesses. Witnesses may be the most objective sources of information, but the accuracy of what they saw or experienced must be critically evaluated. Often a witness may have only witnessed an anomaly in thu functioning of the computer system, but questioning may still result in important information.

- Witnesses without EDP experience may be of limited value when the purpose of the investigation is to aid in development of computer security.

- Management of corporate victims. It is important to identify the appropriate people among management. Different people are appropriate for different types of information. Technical information being the most important, it is best to start with technically oriented management. It is best to ask a person for information only within his area of responsibilities; otherwise the information may be of poor quality and the manager may get into trouble by supplying it. Victims are normally sensitive to the effects of their statements and to the investigator's purposes.

- Individual people are usually not victims in the types of incidents associated with computers.

- Associates of suspects and victims will be a help in interpreting the information from the participants.

- Lawyers who represent the suspects and victims, and public prosecutors are difficult to deal with. Before completion of legal proceedings they are cautious in their statements and afterwards they are usually not interested in the case. They also often attempt to gain information from the investigator and are sizing him up for a possible witness role in the trial. Investigators should avoid being witnesses in trials in order to maintain their neutral positions in meeting with both sides in disputes.

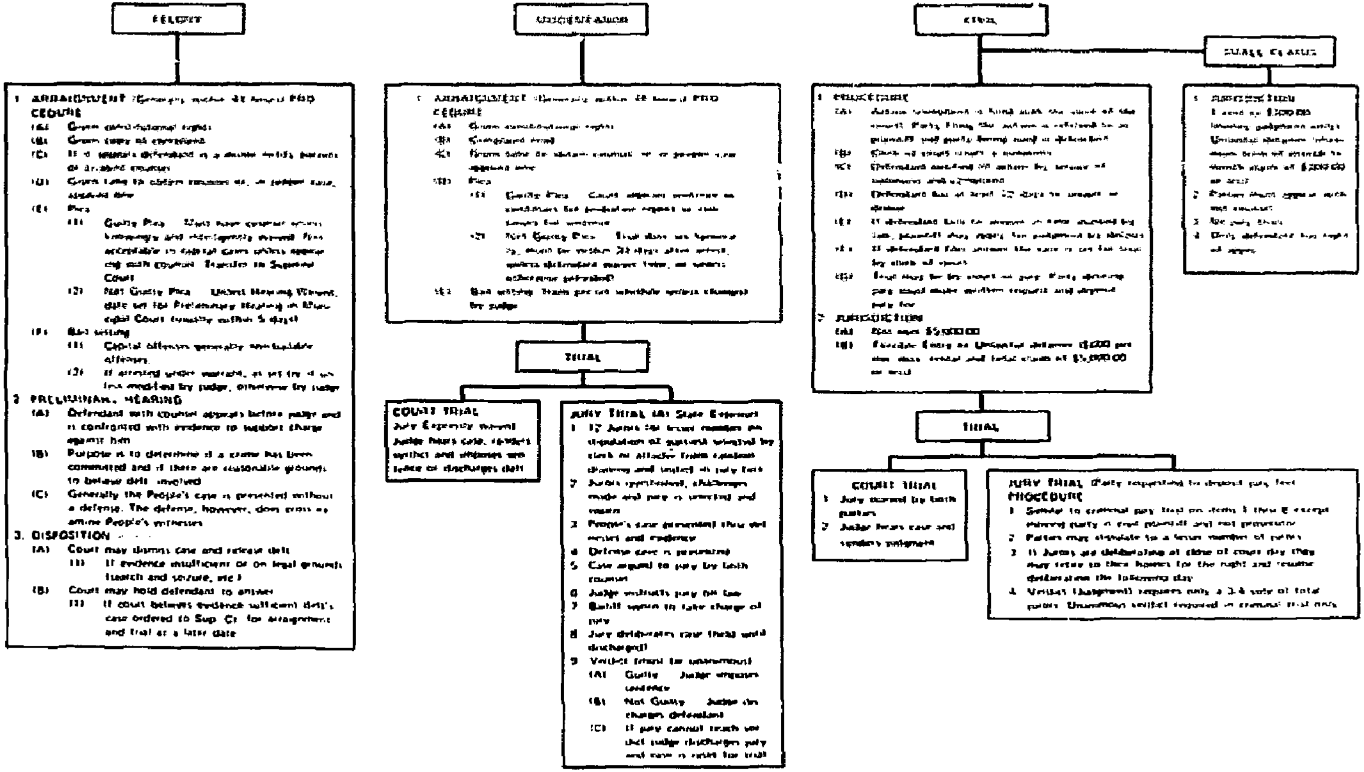
Confidentiality

It is also important to respect confidentiality of sources when requested. A source person should always be explicitly asked to what extent he wishes anonymity, or the information to remain confidential, and confidential to whom. The investigator should explain as much as possible what will be done with the information supplied and with the name of the source.

Timing of Investigations

The best time to investigate a case is immediately after all legal actions or after sanctions or final agreements have been imposed and accepted. Unfortunately, this often takes several years and the value of documenting the case may be reduced. If early investigation is important for research and development of protection measures, problems arise. Although the incident is fresh on the participants' minds, each is protecting and promoting his positions and involvement, and this will last until the case is concluded.

Figure 1 is a diagram showing the sequence of events in legal proceedings.



FELONY

1 ARRAIGNMENT (Generally within 48 hours) PROCEDURE
(A) Given constitutional rights
(B) Given copy of complaint
(C) If a [illegible] defendant is a [illegible], [illegible] of [illegible] counsel
(D) Given time to obtain counsel or, in proper case, assigned one
(E) Plea
(1) Guilty Plea — Must have counsel unless knowingly and intelligently waived. Plea acceptable in capital cases unless appearing with counsel. Transfer to Superior Court
(2) Not Guilty Plea — Unless Hearing Waived, date set for Preliminary Hearing in Municipal Court (usually within 5 days)
(F) Bail setting
(1) Capital offenses generally nonbailable offenses.
(2) If arrested under warrant, as set on it unless modified by judge, otherwise by judge
2 PRELIMINARY HEARING
(A) Defendant with counsel appears before judge and is confronted with evidence to support charge against him
(B) Purpose is to determine if a crime has been committed and if there are reasonable grounds to believe deft. involved
(C) Generally the People's case is presented without a defense. The defense, however, does cross examine People's witnesses
3. DISPOSITION
(A) Court may dismiss case and release deft.
(1) If evidence insufficient or on legal grounds (search and seizure, etc.)
(B) Court may hold defendant to answer
(1) If court believes evidence sufficient deft's case ordered to Sup. Ct. for arraignment and trial at a later date

MISDEMEANOR

1 ARRAIGNMENT (Generally within 48 hours) PROCEDURE
(A) Given constitutional rights
(B) Complaint read
(C) Given time to obtain counsel or in proper case appointed one
(D) Plea
(1) Guilty Plea — Court imposes sentence or continues for probation report or sets time for sentence
(2) Not Guilty Plea — Trial date set (generally, must be within 30 days after arrest, unless defendant waives time, or unless otherwise provided)
(E) Bail setting. Bail per bail schedule unless changed by judge

TRIAL

COURT TRIAL
Jury Expressly Waived. Judge hears case, renders verdict and imposes sentence or discharges deft.

JURY TRIAL (At State Expense)
1 12 Jurors (or lesser number on stipulation of parties) selected by clerk or officer from random drawing and seated in jury box
2 Jurors questioned, challenges made and jury is selected and sworn
3 People's case presented thru witnesses and evidence
4 Defense case is presented
5 Case argued to jury by both counsel
6 Judge instructs jury on law
7 Bailiff sworn to take charge of jury
8 Jury deliberates case (held until discharged)
9 Verdict (must be unanimous)
(A) Guilty — Judge imposes sentence
(B) Not Guilty — Judge discharges defendant
(C) If jury cannot reach verdict judge discharges jury and case is reset for trial

CIVIL

1 PROCEDURE
(A) Action commenced is filed with the clerk of the court. Party filing the action is referred to as plaintiff and party being sued is defendant
(B) Clerk of court issues a summons
(C) Defendant notified of action by service of summons and complaint
(D) Defendant has at least 30 days to answer or demur
(E) If defendant fails to answer in time allowed by law, plaintiff may apply for judgment by default
(F) If defendant files answer the case is set for trial by clerk of court
(G) Trial may be by court or jury. Party desiring jury must make written request and deposit jury fee
2 JURISDICTION
(A) Not over $5,000.00
(B) Forcible Entry or Unlawful detainer ($[illegible] per day rental) and total claim of $5,000.00 or less

SMALL CLAIMS

1 JURISDICTION
Limit of $500.00 (money judgment only). Unlawful detainer (where [illegible] is [illegible] month rent of $[illegible] or less)
2 Parties must appear without counsel
3 No jury trial
4 Only defendant has right of appeal

TRIAL

COURT TRIAL
1 Jury waived by both parties
2 Judge hears case and renders judgment

JURY TRIAL (Party requesting to deposit jury fee)
PROCEDURE
1 Similar to criminal jury trial on items 1 thru 8 except moving party is plaintiff and not prosecutor
2 Parties may stipulate to a lesser number of jurors
3 If Jurors are deliberating at close of court day they may retire to their homes for the night and resume deliberations the following day
4 Verdict (Judgment) requires only a 3/4 vote of total jurors. Unanimous verdict required in criminal trial only

SOURCE: Bancroft-Whitney Co., San Francisco, California

SR 2104 1

FIGURE 1 SEQUENCE OF LEGAL PROCEEDINGS

Investigative Methodology

It is important to find out as much as possible about the suspected or known perpetrator. Because the suspect is the threat we are trying to protect a system from, the interviewer must discover the suspect's knowledge, skills, and access to the target, which enabled him to perform the act. This appears to be the best way to reach the goal of limiting the population of potential perpetrator and then making computer systems as invulnerable as possible against them. An effective study of perpetrators could reveal how best to distribute limited protective resources.

Goals

The goals of investigation are:

- Discover the purpose of the act.
- Discover methods used to perpetrate the act.
- Determine security features and the environment that was violated.
- Determine the circumstances and methods of detection.
- Determine recovery actions.
- Discover the roles of participants and their individual actions.
- Document the results of investigation in complete and useful ways.

A mechanism to help in achieving these goals has been developed in the form of a questionnaire. It first serves the purpose of a checklist, then a documentation aid, and finally a reference document in completed form to be filed. The questionnaire should not be used directly during an interview because it forces an unnatural and rigid structure on interviews that has been found to be unproductive and impractical; instead, it should be used to document the case from material collected and interview notes.

Preparing for Interviews

Preparation for conducting interviews can be done by writing brief cues on note-taking paper for statements the interviewer wants to make and for information he wants to obtain. The questionnaire provides a check-list of items for this purpose. Numerous schemes can be used to direct the interview. A time-sequenced interview will order subjects on the time sequence in which the activities took place. Another method is to elicit the most important items first. The most productive interview, however, should progress in two dimensions:

- In chronological progression of events
- From the general to the specific.

In any case, it is important to establish the identity, purpose, roles, and constraints of each participant in the interview. The interviewer should also have some form of identification and a consistent statement about his sponsors and the purposes of the interview. A letter written on the sponsor's official letter paper to arrange or confirm the interview is the best means to identify the interviewer and to establish the reason for the interview.

Interviewing the suspect requires a disciplined approach to gain the information required. Ask generic questions before resorting to specific questions. This avoids "leading" him. For example, ask such questions as "What would have stopped you from your planned act?" rather than "If you knew the system timed out on LOGON procedures, would you have given up?"

Characteristics of Perpetrators

Certain characteristics have been detected in white-collar criminals, the most common type of perpetrators. Their acts tend to deviate in only minor ways from accepted behavior of their associates. Perpetrators tend to differentiate between dishonest acts that hurt people and acts that are harmful to organizations; the former acts are seen as immoral, but the latter can sometimes be rationalized. Perpetrators have often rationalized their acts to the degree of believing they chose an action from among alternatives that would result in the least harm and trouble to the least number of people or in hurting only people or organizations that deserved what they got.

Precautions

A word of caution is necessary here. It is easy for an investigator to sympathize and identify with the perpetrator and think "there but for the grace of God go I!" An effort must be actively exerted to maintain a sense of perspective and values in the presence of a suspect who has expended great effort in rationalizing his acts. A perpetrator can spend more energy rationalizing his act than planning or carrying it out.

Also, there is the danger that an objective, independent investigator will be drawn into the case by these participants who have special interests. On the other hand, the investigator who can offer help and advice to the participants is more likely to gain cooperation from them.

General Recommendations

The following principles summarize the general steps in investigative methodology:

- Begin the investigation as early as possible
- Learn as much as possible about the suspect

- Become known to as many participants/witnesses as possible
- Make thorough preparation for each interview
- Be cautious about involvement
- Prepare to wait long periods of time for crucial information to be revealed.

Questionnaire Description and Usage

The questionnaire is organized in four parts:

(1) Case identification

(2) Environments of the acts

(3) Description of the acts and detection

(4) Suspect investigation.

Several copies of parts (2), (3), or (4) may be required to describe several acts, environments, or suspects in a single case. Items are usually stated in plural. Singular forms should be assumed when appropriate. Right margins of the pages should be left blank for future coding and processing purposes. It may be necessary to fill out the forms without revealing names or clues to names of participants. Code names may be used for consistency from part to part. Only information relevant to the case and purposes of investigation should be entered. Answer spaces to questions that are irrelevant should be left blank. It is expected that in many cases the forms will be sparsely filled in. Also, some redundancy has been built into this questionnaire for validation purposes and to overcome inconsistencies in terminology. Some redundancy is a result of unclear and nonstandard terminology used in computer technology.

It is assumed that the investigators are experts in various aspects of computer technology and security. The questionnaire is to be filled out by investigators trained in the process of on-site and remote investigation of cases. Victims and others involved in the acts, but who may not be expert investigators, may be asked to fill out parts of the questionnaire to the best of their ability. However, the information obtained in this fashion should be used only as an aid in the investigation, and such questionnaires should not be accepted as basis-of-fact documents without review and validation by an investigator.

The appendix to this manual contains two sets of questionnaires documenting actual cases. One case is presented in open, nonconfidential form except for the name and address of the perpetrator. All facts are public knowledge in this case, and most information came from legal documents and trial transcripts. The other case is documented in a confidential manner even though many of the facts are publicly known. However, the charges against the suspect were dropped.

Persons using the questionnaire must be cautioned to avoid recording data that could result in legal actions against them and their employer. For example, do not identify any participants in the case unless their names and the roles they played have been publicly revealed or their written permission has been obtained.

Appendix A

COMPUTER-RELATED INCIDENT QUESTIONNAIRES

Part 1. Case ID 7121

Earliest Date of Act 1/19/71

Date of This Report ~~12/1/72~~

Revised Date 1/18/73

Coding

COMPUTER-RELATED INCIDENT QUESTIONNAIRE

PART 1. CASE IDENTIFICATION

1.1 Case name ISD vs. UCC Program Theft

1.2 Brief case description An employee of UCC used a UCC RJE terminal and public telephone circuits to steal a listing of a program stored in the ISD computer and alleged to be a trade secret of ISD.

1.3 Key words extracted from 1.2

Employee	RJE terminal	telephone	trade secret
program	steal		

1.4 Names of computer systems involved (operating organization and generic type)

ISD UNIVAC 1108

1.5 Case locations. Cities and local sites of acts, targets, perpetrators

Palo Alto, CA, University Computing, site of the act. Oakland, CA, Information System Design, location of stolen program

1.6 Participants. Victims, suspected perpetrators, prosecutors, witnesses

	Role played	Name	Title, Address, Telephone
A	Victim	ISD	7817 Oakport Rd., Oakland 94621 562-4204
B	Perpetrator	UCC	260 Sheridan Ave., Palo Alto 328-2050
C	Perpetrator		
D	Accuser		President, ISD
E	Prosecutor	Charles Herbert	Alameda County Deputy District Attorney

Case ID 7121

1.7 Type of investigation and sources. Identify all applicable items by inserting names of sources and dates

		Dates
On-site investigation	UCC, ISD, courts of law	3/3/71-8/22/72
Telephone calls	UCC, ISD, attorney	"
Letter correspondence	attorneys	"
Face-to-face interview	C, D, police, attorneys, E, ISD, UCC employees,	"
Directly quoted	C, D, police, ISD, UCC employees	"
Document extraction		

1.8 Authors of this questionnaire Donn B. Parker

Revision by Donn B. Parker

1.9 Case investigators Donn B. Parker

1.10

Case documents	Location
Complaint	Parker files, SRI
Search warrant	"
Depositions	"
Trial proceedings	"
Judge's opinion	"
Newspaper clippings	"
Investigator's notes	"

Case ID 7121

COMPUTER-RELATED INCIDENT QUESTIONNAIRE

PART 2. ENVIRONMENTS OF THE ACT

2.1 Computer systems involved in the case. (Use one form for each system)

2.1.1 System identification ISD UNIVAC 1108

Operating Organization	Facility Locations	CPU Vendor, Model, Storage	Mode of Operation	Purposes
ISD	Oakland	UNIVAC 1108, 64K	Batch, remote access	Commercial computer services

2.1.2 Peripherals pertinent to the case 22m words Fastrand drum storage, card punch, magnetic tape drives.

2.1.3 Operating system, options, modifications, add-ons ISD-modified UNIVAC EXEC II

2.1.4 Software packages pertinent to the case PLOT/TRANS file containing programs PPTGEN, PLTRNS, PLTGEN (515 lines of FORTRAN code)

2.1.5 Terminals pertinent to the case

No.	Make	Model	Location	Ownership	Purposes
	UNIVAC	1004	various customer sites		RJE
1	Calcomp/AT&T	201 D	Modem, Calcomp	633 Plotter,	621 Receiver
1	COPE	36	Palo Alto	UCC	RJE

2.1.6 Communication system (multiplexers, concentrators, circuit types, and their locations) dial-up circuits

2.1.7 Type of computer system application. (Circle letters. More than one type may apply at different times.) a. Transaction system. b. More than one transaction subsystem. c. Transaction subsystems and programmer access. [✓ d.] Programmer access at application language level. [✓ e.] Programmer acces at machine language level. f. Other

2.1.8 Type of access authorization control. (Circle letters. More than one type may apply at different times.) a. None. [✓ b.] Centralized authority granting. c. More than one can grant authority. d. Individual users can authorize others. e. Other ____

2.1.9 Security levels present. (Circle letters. More than one type may apply at different times.) a. System and contents open to all users. b. Part of system and/or contents requires authorized access and part is open to general access. c. More than one level of authorized access in addition to general access. d. More than one level of authorized access and no part is open to general access. [✓ e.] All access must be authorized. f. Other ____

2.1.10 Degrees of confidentiality of the contents of the system. (Circle all appropriate letters.) a. U.S. Government classified (national security). b. Personal or organizational safety (compromise would cause personal unrecoverable injury or death or organizational failure). c. Personal or organizational integrity (unrecoverable injury, damage or loss). [✓ d.] Personal or organizational recoverability (recoverable injury, damage or loss). [✓ e.] Personal or organizational convenience (irritational injury, damage or loss). [✓ f.] Public domain (no confidentiality). g. Other ____

2.1.11 Number of employees dedicated exclusively to computer system protection (Supply numbers). EDP auditors a.____ Guards b. ____ Data validation/control clerks c.____ Other d.____

2.1.12 Staff contacts (operations, systems, applications, hardware maintenance, EDP audit, security) ISD: Robert Larribou. UCC: Jerry Gaylor

Case ID 7121

2.2 "Quick-check" system characteristics (Use one set for each system)

System identification ISD 1108

(Circle appropriate numbers)

[✓ 1.] Local batch
[✓ 2.] Remote batch
3. Time-sharing
[✓ 4.] Multiaccess
5. Time-slicing
[✓ 6.] Multiprogrammed
7. Multiprocessors
[✓ 8.] Single mode of operation
9. Multimode, simultaneous
10. Multimode, sequential
11. Network-connected
12. Hierarchically-connected, head end
13. Hierarchically-connected, subsystem
[✓ 14.] Data communications used
[✓ 15.] Multiplexers on-site
16. Remote Multiplexers
17. Concentrators on-site
18. Remote concentrators
19. High speed circuits (≥9600 bps)
[✓ 20.] Low speed circuits (<9600 bps)
[✓ 21.] Dial-up circuits
22. Private circuits
[✓ 23.] Leased circuits
24. Microwave
25. Half duplex
26. Full duplex
27. Synchronous
28. Asynchronous
29. Conversational terminals
[✓ 30.] Batch or job terminals
31. Transaction terminals
[✓ 32.] Graphics terminals
33. Telemetry terminals
34. Real-time, process control terminals
35. Conversational terminal response
36. Performance monitoring devices
[✓ 37.] Tape drives
38. Disk drives, permanent
39. Disk drives, removable
[✓ 40.] Magnetic drums
41. Add-on core storage
[✓ 42.] Paper tape
43. Mass storage, optical
44. Multivendor central configuration
45. Paged storage, hardware
46. Paged storage, software
47. Virtual storage, hardware
48. Virtual storage, software
49. Relocation feature
50. Hardware storage protection
51. Privileged instructions
[✓ 52.] Continuous operation
53. First shift only
54. Two shifts
55. Three shifts
[✓ 56.] Weekend, holiday operation
57. Dedicated to one (few) applications
58. Business applications
[✓ 59.] Engineering applications
[✓ 60.] Research applications
61. Integrated file applications
62. Process control applications
63. Transaction applications
64. U.S. Government classified processing

Case ID 7121

65. All access local to system
[✓ 66.] Multiple customers (corporations)
[✓ 67.] Service bureau operation
68. Operation shared with other companies
69. Operation by a service company
70. Maintenance by CPU vendor
71. Maintenance by independent service
72. Multivendor maintenance
73. In-house maintenance
[✓ 74.] CPU-vendor supplied operating system
75. Independent vendor operating system
76. In-house operating system
[✓ 77.] Modified vendor operating system
78. More than one operating system used
[✓ 79.] On-line user-program library
[✓ 80.] On-line application files
81. Files encrypted
[✓ 82.] Data encryption optional
83. Data communication hardware encryption
84. Data communication software encryption
85. Terminal identification by hardware

Terminal LOGON by

86. User ID
87. Password
88. Single-use password
[✓ 89.] Account code
[✓ 90.] Site code
91. Dialog with user
92. Time limit
93. Error limit
94. Portable key or card

95. Security features integrated in OS
96. Security features added on
97. Security features in isolated modules
[✓ 98.] Centralized access authorization
99. Decentralized access authorization
100. OS isolated from users
101. Users' jobs isolated from each other
[✓ 102.] File access restricted by authorization
103. First write before read data protection
104. Storage erasure after use
105. I/O buffers, registers cleared after use
106. Access authorization data in files
107. Access authorization in file index tables
[✓ 108.] User access to assembly-level language
[✓ 109.] File activity tracing or auditing
110. Security monitoring of system use
111. Real-time human monitoring of security
112. Console dedicated to security functions

Remote back-up storage of

113. Operating system
114. Application programs
115. Data files

116. Removable storage devices stored local to drives
117. Positive door access control to facilities
118. Programmers' and operators' work areas separated

Case ID 7121

COMPUTER-RELATED INCIDENT QUESTIONNAIRE

PART 3. DESCRIPTION OF THE ACTS AND DETECTION

3.1 Type of act. (Circle applicable letters)

[✓ a.] Unauthorized use of the services of computer systems.

b. Unauthorized sale of the services of computer systems.

[✓ c.] Unauthorized taking of information, computer programs or property or copies thereof.

d. Direct financial gain by taking negotiable instruments or transferring monetary credit.

e. Vandalism.

f. Other ______________________________

____

3.2 Access and methods used to perpetrate the acts

3.2.1 Is physical access to the sites of the acts applicable and pertinent to this case? yes [✓ no]

3.2.2 Physical access: times and days ______________________________

(Circle appropriate letters and prefix capital letters to identify suspects)

___a. Covert access. ___b. Overt access. ___c. Authorized. ___d. Unauthorized. ___e. Assisted by others. ___f. Tools or devices used to gain entry. ___g. Observed by others. ___h. Impersonation used. ___i. Access reported to responsible persons. When? ______________________________

____

___j. Diversion tactics used. Describe ______________________________

____

3.2.3 Were the sites of the acts protected by: (Circle appropriate letters)

a. Locked doors. b. Guards. c. Electronic/optical devices. [✓ d.] Not protected. Describe ______________________________

____

3.2.4 Methods and devices used: (Circle appropriate numbers and prefix capital letters to identify suspects) C[✓ 1.] On-line. ___2. Off-line. ___3. Conversational terminal. ___4. Transaction terminal. C[✓ 5.] Job entry terminal. ___6. Computer console. ___7. Security console. ___8. Supervisory terminal. ___9. Maintenance console. ___10. Direct manual action. ___11. By issuing instructions to other people.

Case ID 7121

___12. Off-line program manipulation. ___13. Off-line job control manipulation. C [✓ 14.] Terminal commands. C [✓ 15.] Immediate results. ___16. Delayed results. ___17. On-line program manipulation. C [✓ 18.] By impersonation. ___19. Program impersonation. ___20. Operating system penetration. ___21. Violation of program boundaries. ___22. Violation of data storage boundaries. ___23. Violation of parameter value ranges. ___24. Simulation of an authorized function. ___25. Covert. C [✓ 26.] Overt. ___27. New program. ___28. Existing program. C [✓ 29.] Utility program. C [✓ 30.] Unauthorized use of identification codes. ___31. Covert use of communication circuits. ___32. Disguised as an accident. ___33. Accident or error used. ___34. Overloading of a system activity. ___35. Overloading of a manual activity. ___36. Diversion used. ___37. Input data manipulation. ___38. Output modification. ___39. Subversion of protective features. ___40. Procedural modification. ___41. System breakdown (crash) necessary for perpetration of the act. C [✓ 42.] Standard operating procedures used. ___43. Non-standard operating procedures used. ___44. Information, programs or property taken from a person by force. ___45. Information, programs or property taken from a person by deception. ___46. Other

3.2.5 Narrative description of methods and devices used. Authorized use of a COPE 36 RJE terminal at UCC simulating a UNIVAC 1004. Access to the ISD 1108 gained by unauthorized use of an unlisted telephone number, account code and site code, all obtained from a mutual customer's site. Job cards were entered from the terminal to request punch card output of a file PLOT/TRANS, but cards were punched at ISD rather than at the terminal. Name of the file was obtained from another mutual customer. A listing of the file was then obtained at the UCC terminal and carried to the perpetrator's office.

3.2.6 Key words used above: authorized COPE 36 RJE terminal UNIVAC 1004
unauthorized telephone account code site code
punch card listing job cards file

Case ID 7121

3.3 Goals, Targets and Results

	a. Unauthorized removal	b. Unauthorized usage	c. Used in unintended ways	d. Unauthorized removal of a copy	e. Unauthorized modification	f. Total destruction	g. Reparable damage	h. Not achieved	i. Achieved partially	j. Achieved totally	k. Results unintended by suspects
3.3.1 Hardware											
1. CPU		C								C	
2. Storage		C								C	
3. Channels		C								C	
4. Controllers		C								C	
5. Peripherals		C								C	
6. Cables		C								C	
7. Terminals										C	
8. Communications devices		C								C	
9. Communication circuits		C								C	
10. Parts inventory											
11. Monitoring devices											
12. Security devices											
13. Other ________________											
________________											
3.3.2 Media											
15. Disk packs											
16. Magnetic tape (mini or cassette)											
17. Paper tape											
18. Punch cards		C						C			C
19. Film											
20. Printer paper, carbon paper											
21. Printer ribbons											
22. Other ________________											

Case ID 7121

3.3.3 Software

	a. Unauthorized removal	b. Unauthorized usage	c. Used in unintended ways	d. Unauthorized removal of a copy	e. Unauthorized modification	f. Total destruction	g. Reparable damage	h. Not achieved	i. Achieved partially	j. Achieved totally	k. Results unintended by suspects
22. Application programs											
23. System of application programs											
24. Library of application programs											
25. Job control instructions		C							C		C
26. Operating system		C							C		C
27. Supervisor											
28. Job scheduler											
29. Queueing control											
30. Interrupt processor											
31. Job swapper											
32. Resource allocation											
33. Storage manager											
34. I/O processors											
35. Operator control											
36. Accounting											
37. Recovery											
38. System initialization											
39. System bootstrap											
40. Library manager											
41. Job control translator											
42. Terminal manager											
43. Activity monitor											
44. Performance monitor											
45. Access controller											
46. Authorization controller											

Case ID 7121

	a. Unauthorized removal	b. Unauthorized usage	c. Used in unintended ways	d. Unauthorized removal of a copy	e. Unauthorized modification	f. Total destruction	g. Reparable damage	h. Not achieved	i. Achieved partially	j. Achieved totally	k. Results unintended by suspects
47. I/O drivers											
48. Compilers, assemblers, translators											
49. Utility programs				C						C	
50. Other ________________											
________________											
3.3.4 Data											
51. Stored on-line application files											
52. Stored off-line application files											
53. Machine-readable input data											
54. Machine-readable output data											
55. Input data for conversion											
56. Output reports	C									C	
57. Operations records											
58. Active operating system tables, files		C		C						C	
59. Security authorization tables											
60. User identification tables											
61. System monitoring files											
62. Buffer files											
63. Queueing files											
64. Other ________________											
________________											
3.3.5 Documents											
65. System software manuals											
66. System user manuals											

Case ID 7121

	a. Unauthorized removal	b. Unauthorized usage	c. Used in unintended ways	d. Unauthorized removal of a copy	e. Unauthorized modification	f. Total destruction	g. Reparable damage	h. Not achieved	i. Achieved partially	j. Achieved totally	k. Results unintended by suspects
67. System software specifications											
68. System design documents											
69. System usage aids											
70. System newsletters											
71. Maintenance documents											
72. Hardware manuals											
73. Hardware drawings											
74. Operator instructions											
75. System status reports											
76. Data control instructions											
77. Audit documents											
78. Security documents											
79. Data preparation instructions											
80. Application manuals											
81. Application specifications											
82. Organization procedures, charts											
83. Personnel lists											
84. Published reports, papers											
85. Unpublished reports, papers											
86. Other ____________________											
3.3.6 Facilities											
86. Doors											
87. Windows											
88. Walls											
89. Floors											

Case ID 7121

	a. Unauthorized removal	b. Unauthorized usage	c. Used in unintended ways	d. Unauthorized removal of a copy	e. Unauthorized modification	f. Total destruction	g. Reparable damage	h. Not achieved	i. Achieved partially	j. Achieved totally	k. Results unintended by suspects
90. Ceilings											
91. Locks											
92. Safety equipment											
93. Power supply											
94. Oral communication equipment											
95. Air conditioning equipment											
96. Lights											
97. Security alarms											
98. TV equipment											
99. Photographic equipment											
100. Furniture											
101. Furnishings											
102. Data keying devices											
103. Off-line processors											
104. Other ______________											
______________											

3.4 Actions taken by suspects to avoid detection (Insert capital letters to identify participants).

	Restore a.	Change b.	Destroy c.	Remove d.	Contributed to Detection e.
1. System logs					A
2. Security log					
3. Program changes					
4. Data changes					
5. Label or name changes					
6. Programs					
7. Data					
8. Buffer contents					
9. Storage contents					
10. Fingerprints, pictures					
11. Waste materials					
12. Moved equipment					
13. Moved media					A
14. Moved materials					
15. Telephone circuit usage log					A
16. Other ______					
17. ______					

3.4.1 Describe No actions taken to avoid detection

3.4.2 Detection. (Circle appropriate letters) a. Before acts could occur. b. During acts. [✓ c.] After acts, time period 1 month.

[✓ d.] Accidental discovery. e. By established detection methods.

[✓ f.] Suspects identified. [✓ g.] Suspects caught.

3.4.3 Participants in detection and suspect identification. (Use capital letters to identify participants.)

	a. Detection	b. Suspect Identification
1. Computer operations staff		
2. Security staff		
3. Audit staff		
4. Systems programming staff		A
5. Hardware maintenance staff		
6. Applications staff		
7. Janitorial staff		
8. Vendor's staff		
9. System users		
10. Customer support staff	A	A
11. Other ________________		

3.4.4 Describe detection James Vernor, manager of customer support at ISD, accidently found the punch cards at mutual customer's site after delivery there (C had used that customer's account code thus identifying the cards as belonging to customer). The 1108 log showed time the cards were punched. Police obtained the PT&T toll call log identifying UCC. A search at UCC produced the file listing.

3.5 Suspects' positions relative to the acts and systems involved. (Circle appropriate numbers and prefix capital letters to identify suspects.) ___1. Computer system management. ___2. Company management. ___3. Application programmer/analyst. ___4. System designer. ___5. System programmer/analyst. ___6. Program maintenance. ___7. Auditor. ___8. Data clerk. ___9. Security guard. ___10. Building maintenance worker. ___11. Hardware maintenance engineer. ___12. Data conversion operator. ___13. Computer/peripheral operator. ___14. Courier or messenger. ___15. Outside consultant. ___16. Company employee (not in computer system staff). ___17. Vendor's employee, on-site. ___18. Vendor's employee, off-site. ___19. Internal customer of system. ___20. External customer of system. C [✓ 21.] Business competitor's employee. ___22. Business associate employee. ___23. A person involuntarily served or affected by the computer system. ___24. A person voluntarily served or affected by the computer system. ___25. Social or political dissident. ___26. Other ______________________________. ___27. Other ______________________________

Case ID 7121

3.5.1 Knowledge and experience of the suspects. (Identify each suspect by a capital letter. Multiple entries for a single box are acceptable.)

	a. Knowledge	b. Experience	c. Not authorized	d. Authorized	e. Of systems involved in these acts	f. Necessary to accomplish the acts	g. Faulty knowledge or error resulting in failure	h. Faulty knowledge or error resulting in detection
1. Access to facilities								
2. Operation of terminals	C	C	C		C	C		C
3. Operation of peripherals								
4. Operation of communications	C	C	C		C	C		
5. Operation of computer	C	C						
6. Job submission	C	C	C		C	C		C
7. Access identification	C	C	C		C	C		
8. Data submission	C	C						
9. Data preparation	C	C						
10. Data conversion	C	C						
11. Data control	C	C						
12. Application program use	C	C						
13. Application program modification	C	C						
14. Application programming	C	C						
15. Systems programming	C	C						
16. Operating system modification	C	C						
17. Computer modification	C	C						
18. Peripherals modification	C	C						

Case ID 7121

	a. Knowledge	b. Experience	c. Not authorized	d. Authorized	e. Of systems involved in these acts	f. Necessary to accomplish the acts	g. Faulty knowledge or error resulting in failure	h. Faulty knowledge or error resulting in detection
19. Terminals modification	C	C						
20. Communication modification	C	C						
21. Wiretapping								
22. Radiation pickup								
23. System security modification								
24. System auditing								
25. System testing	C	C						
26. Acquainted with staff	C							
27. Acquainted with users/customers	C							
28. Organization procedures								
29. Staff working schedules								
30. System schedules	C							
31. Independent training course								
32. Internal training course								
33. Other ____________								

3.6 Estimate of value of losses, injuries and damages: $ 15,000

3.7 Changes made in the computer system as a result of these acts. Security increased? [✓ yes] no Describe Scrambling program used to encypher all sensitive files.

3.8 Most important implications of this case Theft of programs by remote terminal and telephone. Access knowledge was easily obtained to pose as a legitimate user. Perpetrators' acts were similar to acts of ISD and UCC employees accessing each other's computer on numerous occasions. Legal precedent may be set regarding unauthorized access to commercial services and trade secret protection measures for computer programs.

3.9 Additional information C was convicted of theft of a trade secret, fined $5000 and given a 3 year suspended sentence. Civil damages were awarded to ISD: $2,750 from C and $290,000 from UCC. Appeals may be made.

COMPUTER-RELATED INCIDENT QUESTIONNAIRE

PART 4. SUSPECT INVESTIGATION (One form for each Suspect)

4.1 Interviews

Date	Interviewer	Interviewee	Location
3/3/71-8/22/72	D. B. Parker	C	SRI, UCC, various

4.2 Background

4.2.1 Name C Age 31 Sex M

4.2.2 Home address ----

Telephone ----

4.2.3 Work address UCC, 260 Sheridan Avenue, Palo Alto, CA

Telephone 328-2050

4.2.4 Education (Circle) High school 1 2 3 [✓ 4] years. Location Salt Lake City

College 1 2 3 [✓ 4] years. Locations U.C. Berkeley

Degree	Subject	Institution	Year
BS	EE	U.C. Berkeley	'64

Professional society membership

4.2.5 (Circle appropriate letters) a. Married b. Separated c. Divorced

d. Widowed [✓ e.] Single Children: Age ___ Age ___ Age ___ Age ___

4.2.6 Present employer UCC Years 4

Occupation or title Technical Consultant

Brief job description Customer support and application development.

4.2.7 Other business interests

4.2.8 Salary (Circle a letter) a. less than $6000 b. 6000-7999 c. 8000-9999

d. 10,000-13,999 e. 14,000-17,999 f. 18,000-23,999 g. 24,000-29,999

h. 30,000-39,999 h. 40,000-49,999 i. More than 50,000

4.2.9 Recent employment (Most recent first)

Employer	Position	From	To
Noller Control Systems	System Designer	66	69
Public Health Service	Programmer (Lt.)	64	66
Philco Ford, Palo Alto	Electronic Technician	60	61

Case ID 7121

4.2.10 Criminal history. Number of arrests 1 Number of convictions 1

Arrest Charges	Date	Disposition
Grand theft, theft of a trade secret	2/23/71	Convicted of theft of a trade secret, 12/11/72. $5,000 fine and 3-year probation.

4.3 Suspect's involvement in the incident.

C was directed by management to perform the act. He planned it and carried it out alone. Others at UCC knew of his actions.

4.4 Before the acts

4.4.1 Purpose of the acts (Circle appropriate letters). a. Direct financial gain by acquiring a negotiable instrument or transfer of credit. b. Indirect financial gain by converting results of the acts to financial gain. c. Personal advancement. d. Revenge. e. To support ideals. f. To right a wrong. [✓ g.] A challenge. [✓ h.] Curiosity. i. Self-amusement. j. Amusement of others. [✓ k.] To help somebody else. [✓ l.] Other gain competitive advantage

4.4.2 Source of the idea for perpetrating the acts. (Circle appropriate letters.) a. Accident or error demonstrated the possibilities. [✓ b.] Learned of similar acts. [✓ c.] Had performed similar acts. [✓ d.] Associates or friends performed similar acts. [✓ e.] Associates or friends talked about similar acts. [✓ f.] Exposure of the target represented a temptation. [✓ g.] Apparent ease of the acts represented a temptation. h. Other

4.4.3 Attitude of the suspect towards potential individual, personal victims, if any. (Circle appropriate letters) [✓ a.] Sorry. b. Sympathetic. c. Hostile. [✓ d.] Superior to them. e. Inferior to them. f. Indifferent. g. Other

4.4.5 Other similar acts suspect was aware of.

Act	Source
Taking information from and running benchmark tests in ISD and UCC computers.	Civil case transcript
C had been authorized by ISD to access the ISD computer previously.	"

4.4.6 Planning. (Circle appropriate letters) a. Acts were not planned. b. Acts were partially planned. [✓ c.] Acts were completely planned. d. Planning was a full time effort. [✓ e.] Planning was a part time effort. f. Cost of the acts was estimated. g. Risk was evaluated. h. Sanctions if caught were known. [✓ i.] Avoidance of discovery was planned. j. Discovery was expected after the acts were perpetrated. [✓ k.] If caught, exposure to family, friends or associates was feared. [✓ l.] If caught, public exposure was feared. [✓ m.] Certain of carrying out plans. n. Uncertain of carrying out plans. o. Would be successful even though caught or exposed. [✓ p.] Would not be successful if caught or exposed. [✓ q.] Confident of success. r. Not confident of success. [✓ s.] Was not aware of criminal nature of the acts. t. Was not aware of unethical, unfair or immoral nature of the acts. [✓ u.] A change in protection of the system could have aborted plans. v. New knowledge required. [✓ w.] New knowledge not required. x. New skills required. [✓ y.] New skills not required. [✓ z.] Planning included other participants. * Act planned from a position of trust.

4.4.7 New skills acquired None

4.4.8 New knowledge acquired None

4.4.9 Collusion (Place an asterisk before name of the planning leader if not the suspect)

Name	Relationship to Suspect	Nature of Involvement

4.4.10 Date act was first conceived 1/19/71

By whom C

4.4.11 Planning period. From 1/19/71 to

4.5 During the acts

4.5.1 Period of time to conduct the acts (date, time). From 1/19/71 6 p.m. to 6:30 p.m.

4.5.2 Actions (Circle appropriate letters) a. Compulsive. b. Frightened. [✓ c.] Confident. [✓ d.] Methodical. e. Disorganized. [✓ f.] Followed plans. g. Deviated from plans. [✓ h.] Encountered unexpected situations. i. Aware of witnesses. j. Careful to remove evidence. [✓ k.] Not concerned with evidence. [✓ l.] In collusion with others. m. No collusion. n. Required cooperation of innocent people. [✓ o.] No cooperation of others required. [✓ p.] Actions were against a system. q. Actions were against people. [✓ r.] Posed or disguised as somebody else. s. Acted under his own identity. t. Fearful of detection. [✓ u.] Not fearful of detection. v. Successful. [✓ w.] Partially successful. x. Not successful.

4.5.3 Collusion in the acts (Place an asterisk before name of the leader if not the suspect)

Name	Relationship to Suspect	Nature of Involvement

4.5.4 Witnesses

Name	Relationship to Suspect	Nature of Involvement

4.5.5 Suspect disguised or posed as User at mutual customer's site.

4.5.6 Mistakes and deviation from plans C requested punch cards not knowing they are produced at ISD rather than at his terminal.

4.5.7 Reasons for success or failure Detailed knowledge of system at ISD b t failed to remember punch card service limitations.

4.6 After the acts

4.6.1 (Circle appropriate letters) [✓ a.] Eager to discuss his actions. b. Willing to discuss his actions. c. Unwilling to supply information. [✓ d.] Left the scene of his actions normally. e. Left the scene in haste or abnormally.

f. Sees himself as a hero. [✓ g.] Is remorseful. h. Is self-righteous. i. Is indifferent. j. Is elated. [✓ k.] Shows animosity toward victims. [✓ l.] Shows animosity toward other involved parties. m. Believes his actions were appropriate for the circumstances. [✓ n.] Feels he was wrong in his actions. o. Would repeat the actions under similar circumstances. [✓ p.] Would never repeat his actions. [✓ q.] Willing to make restitution. r. Not willing to make restitution. s. Feels he made a net gain towards his objectives. [✓ t.] Suffered a net loss towards his objectives.

4.6.2 What did the suspect fear most (Rank by numbers or leave blank if not applicable)

[✓ a.] ___ Discovery of the act

b. ___ Exposure of him as the perpetrator

c. ___ Harm to others

d. ___ Punishment

e. ___ Publicity

f. ___ Other ______

g. ___ Other ______

4.6.3 Feelings towards other involved parties

Name	Feelings
Prosecutors	Unfair use as a test case of a new law

4.6.4 What circumstances would have stopped the suspect's actions? If C's management had not insisted he get a copy of the program that day. Another copy would have been available the next day. Proprietary identification of the file would have stopped C.

4.6.5 Alternative actions suspect could have taken:

Action	Reason for Rejection
Wait to get a copy another way.	C was urged by management to get a copy even though he didn't think he needed it.
Become convinced UCC didn't need a copy.	

Part 1. Case ID 7042 | Coding

Earliest Date of Act 5/28/70

Date of This Report 12/14/72

Revised Date

COMPUTER-RELATED INCIDENT QUESTIONNAIRE

PART 1. CASE IDENTIFICATION

1.1 Case name Assigned GO TO

1.2 Brief case description Unauthorized terminal access to the operating system of a commercial time-sharing service via leased telephone line by a former customer and systems programmer employee of the service firm. System files were taken and numerous crashes caused.

1.3 Key words extracted from 1.2

unauthorized	terminal	operating system	time-sharing
telephone	employee	customer	crashes

1.4 Names of computer systems involved (operating organization and generic type)

GE 400 time-sharing system

1.5 Case locations. Cities and local sites of acts, targets, perpetrators

1.6 Participants. Victims, suspected perpetrators, prosecutors, witnesses

	Role played	Name	Title, Address, Telephone
A	Victim		Time-sharing company
B	Suspect		Customer
C	Suspect		Systems programmer employee
D	Prosecutor	Byron Trapp	Ass't U.S. Attorney, Post Office Building, Cincinnati 45202
E			

Case ID 7042

1.7 Type of investigation and sources. Identify all applicable items by inserting names of sources and dates

		Dates
On-site investigation	A	12/14/72
Telephone calls	A, B	11/27/72
Letter correspondence	A, B, D	11/72, 4/17/72
Face-to-face interview	A	12/14/72
Directly quoted	A, B	12/14/72
Document extraction	News clippings	
	terminal printout	12/14/72

1.8 Authors of this questionnaire Donn B. Parker

Revision by

1.9 Case investigators Donn B. Parker

1.10

Case documents	Location
Computerworld articles	Parker case file
Terminal printout of penetration example	"
Letter: Trapp to Parker 4/27/71	"
Letters: Parker to Trapp, A, B	"

Case ID 7042

COMPUTER-RELATED INCIDENT QUESTIONNAIRE

PART 2. ENVIRONMENTS OF THE ACT

2.1 Computer systems involved in the case. (Use one form for each system)

2.1.1 System identification A's GE 400

Operating Organization	Facility Locations	CPU Vendor, Model, Storage	Mode of Operation	Purposes
A	City of A	GE 400	Time-sharing	Commercial service

2.1.2 Peripherals pertinent to the case

2.1.3 Operating system, options, modifications, add-ons

GE 400 time-sharing system modified by A

2.1.4 Software packages pertinent to the case Fortran compiler, system utilities

2.1.5 Terminals pertinent to the case

No.	Make	Model	Location	Ownership	Purposes
	Teletype	33, 35	City of B	B's employer	Time-sharing

2.1.6 Communication system (multiplexers, concentrators, circuit types, and their locations) Multiplexer in B's city, operated by C, leased long line to A's city, concentrator in A's city

2.1.7 Type of computer system application. (Circle letters. More than one type may apply at different times.) a. Transaction system. b. More than one transaction subsystem. c. Transaction subsystems and programmer access. [✓ d.] Programmer access at application language level. e. Programmer access at machine language level. f. Other

Case ID 7042

2.1.8 Type of access authorization control. (Circle letters. More than one type may apply at different times.) a. None. [✓ b.] Centralized authority granting. c. More than one can grant authority. [✓ d.] Individual users can authorize others. e. Other ______________________________

2.1.9 Security levels present. (Circle letters. More than one type may apply at different times.) a. System and contents open to all users. b. Part of system and/or contents requires authorized access and part is open to general access. c. More than one level of authorized access in addition to general access. [✓ d.] More than one level of authorized access and no part is open to general access. [✓ e.] All access must be authorized. f. Other ______________________________

2.1.10 Degrees of confidentiality of the contents of the system. (Circle all appropriate letters.) a. U.S. Government classified (national security). b. Personal or organizational safety (compromise would cause personal unrecoverable injury or death or organizational failure). [✓ c.] Personal or organizational integrity (unrecoverable injury, damage or loss). [✓ d.] Personal or organizational recoverability (recoverable injury, damage or loss). [✓ e.] Personal or organizational convenience (irritational injury, damage or loss). f. Public domain (no confidentiality). g. Other ______

2.1.11 Number of employees dedicated exclusively to computer system protection (Supply numbers). EDP auditors a.______ Guards b. ______ Data validation/ control clerks c.______ Other d.______________________________

2.1.12 Staff contacts (operations, systems, applications, hardware maintenance, EDP audit, security) A______________________________

____

____

____

Case ID7042

2.2 "Quick-check" system characteristics (Use one set for each system)

System identification A's GE 400

(Circle appropriate numbers)

1. Local batch
2. Remote batch
[✓ 3.] Time-sharing
[✓ 4.] Multiaccess
[✓ 5.] Time-slicing
6. Multiprogrammed
7. Multiprocessors
[✓ 8.] Single mode of operation
9. Multimode, simultaneous
10. Multimode, sequential
11. Network-connected
12. Hierarchically-connected, head end
13. Hierarchically-connected, subsystem
[✓ 14.] Data communications used
[✓ 15.] Multiplexers on-site
16. Remote Multiplexers
17. Concentrators on-site
[✓ 18.] Remote concentrators
19. High speed circuits (≥9600 bps)
[✓ 20.] Low speed circuits (<9600 bps)
[✓ 21.] Dial-up circuits
22. Private circuits
[✓ 23.] Leased circuits
24. Microwave
25. Half duplex
26. Full duplex
27. Synchronous
28. Asynchronous
[✓ 29.] Conversational terminals
30. Batch or job terminals
31. Transaction terminals
32. Graphics terminals
33. Telemetry terminals
34. Real-time, process control terminals
[✓ 35.] Conversational terminal response
36. Performance monitoring devices
37. Tape drives
38. Disk drives, permanent
[✓ 39.] Disk drives, removable
40. Magnetic drums
41. Add-on core storage
42. Paper tape
43. Mass storage, optical
44. Multivendor central configuration
45. Paged storage, hardware
46. Paged storage, software
47. Virtual storage, hardware
48. Virtual storage, software
49. Relocation feature
50. Hardware storage protection
51. Privileged instructions
[✓ 52.] Continuous operation
53. First shift only
54. Two shifts
55. Three shifts
56. Weekend, holiday operation
57. Dedicated to one (few) applications
[✓ 58.] Business applications
[✓ 59.] Engineering applications
[✓ 60.] Research applications
61. Integrated file applications
62. Process control applications
63. Transaction applications
64. U.S. Government classified processing

Case ID 7042

65. All access local to system
[✓ 66.] Multiple customers (corporations)
[✓ 67.] Service bureau operation
68. Operation shared with other companies
69. Operation by a service company
[✓ 70.] Maintenance by CPU vendor
71. Maintenance by independent service
72. Multivendor maintenance
73. In-house maintenance
[✓ 74.] CPU-vendor supplied operating system
75. Independent vendor operating system
76. In-house operating system
[✓ 77.] Modified vendor operating system
78. More than one operating system used
[✓ 79.] On-line user-program library
[✓ 80.] On-line application files
81. Files encrypted
82. Data encryption optional
83. Data communication hardware encryption
84. Data communication software encryption
[✓ 85.] Terminal identification by hardware

Terminal LOGON by

[✓ 86.] User ID
[✓ 87.] Password
88. Single-use password
[✓ 89.] Account code
[✓ 90.] Site code
91. Dialog with user
92. Time limit
[✓ 93.] Error limit
94. Portable key or card

95. Security features integrated in OS
96. Security features added on
97. Security features in isolated modules
[✓ 98.] Centralized access authorization

99. Decentralized access authorization
[✓ 100.] OS isolated from users
[✓ 101.] Users' jobs isolated from each other
[✓ 102.] File access restricted by authorization
103. First write before read data protection
104. Storage erasure after use
105. I/O buffers, registers cleared after use
106. Access authorization data in files
[✓ 107.] Access authorization in file index tables
108. User access to assembly-level language
109. File activity tracing or auditing
110. Security monitoring of system use
111. Real-time human monitoring of security
112. Console dedicated to security functions

Remote back-up storage of

[✓ 113.] Operating system
[✓ 114.] Application programs
[✓ 115.] Data files

116. Removable storage devices stored local to drives
117. Positive door access control to facilities
118. Programmers' and operators' work areas separated

Case ID 7042

COMPUTER-RELATED INCIDENT QUESTIONNAIRE

PART 3. DESCRIPTION OF THE ACTS AND DETECTION

3.1 Type of act. (Circle applicable letters)

[✓ a.] Unauthorized use of the services of computer systems.

b. Unauthorized sale of the services of computer systems.

[✓ c.] Unauthorized taking of information, computer programs or property or copies thereof.

d. Direct financial gain by taking negotiable instruments or transferring monetary credit.

[✓ e.] Vandalism.

f. Other ______________________________

3.2 Access and methods used to perpetrate the acts

3.2.1 Is physical access to the sites of the acts applicable and pertinent to this case? [✓ yes] no

3.2.2 Physical access: times and days various

(Circle appropriate letters and prefix capital letters to identify suspects)

___a. Covert access. C [✓ b.] Overt access. C [✓ c.] Authorized.

___d. Unauthorized. ___e. Assisted by others. ___f. Tools or devices used to gain entry. C [✓ g.] Observed by others. ___h. Impersonation used.

___i. Access reported to responsible persons. When? ______________________________

___j. Diversion tactics used. Describe ______________________________

3.2.3 Were the sites of the acts protected by: (Circle appropriate letters)

[✓ a.] Locked doors. b. Guards. c. Electronic/optical devices. d. Not protected. Describe ______________________________

3.2.4 Methods and devices used: (Circle appropriate numbers and prefix capital letters to identify suspects) B [✓ 1.] On-line. ___2. Off-line. B [✓ 3.] Conversational terminal. ___4. Transaction terminal. ___5. Job entry terminal. ___6. Computer console. ___7. Security console. ___8. Supervisory terminal. ___9. Maintenance console. ___10. Direct manual action. ___11. By issuing instructions to other people.

Case ID 7042

___12. Off-line program manipulation. ___13. Off-line job control
manipulation. B [✓ 14.] Terminal commands. B [✓ 15.] Immediate results.
___16. Delayed results. B [✓ 17.] On-line program manipulation.
B [✓ 18.] By impersonation. ___19. Program impersonation. B [✓ 20.] Operating
system penetration. B [✓ 21.] Violation of program boundaries.
___22. Violation of data storage boundaries. B [✓ 23.] Violation of
parameter value ranges. ___24. Simulation of an authorized function.
B [✓ 25.] Covert. ___26. Overt. B [✓ 27.] New program. ___28. Existing
program. B [✓ 29.] Utility program. B [✓ 30.] Unauthorized use of identification codes. B [✓ 31.] Covert use of communication circuits.
___32. Disguised as an accident. ___33. Accident or error used.
___34. Overloading of a system activity. ___35. Overloading of a manual
activity. ___36. Diversion used. ___37. Input data manipulation.
___38. Output modification. B [✓ 39.] Subversion of protective features.
___40. Procedural modification. ___41. System breakdown (crash) necessary
for perpetration of the act. B [✓ 42.] Standard operating procedures used.
B [✓ 43.] Non-standard operating procedures used. ___44. Information,
programs or property taken from a person by force. ___45. Information,
programs or property taken from a person by deception. ___46. Other

3.2.5 Narrative description of methods and devices used. Access was made using
known passwords and capture of a leased line. Fortran allowed execution of
an assigned GO TO transferring control to user's COMMON where data was
executed that referenced an illegal address. This caused an interrupt at
which point the operating system was captured in Master Mode. System and
user files were obtained and the system was crashed on numerous occasions.

3.2.6 Key words used above: passwords ___ Fortran ___ GO TO
COMMON ___ illegal address ___ interrupt ___ operating system
Master Mode ___ user files ___ crashed

Case ID 7042

3.3 Goals, Targets and Results

	a. Unauthorized removal	b. Unauthorized usage	c. Used in unintended ways	d. Unauthorized removal of a copy	e. Unauthorized modification	f. Total destruction	g. Reparable damage	h. Not achieved	i. Achieved partially	j. Achieved totally	k. Results unintended by suspects
3.3.1 Hardware											
1. CPU		B								B	
2. Storage		B								B	
3. Channels		B								B	
4. Controllers											
5. Peripherals											
6. Cables											
7. Terminals											
8. Communications devices		B								B	
9. Communication circuits		B								B	
10. Parts inventory											
11. Monitoring devices											
12. Security devices											
13. Other ________________											
________________											
3.3.2 Media											
15. Disk packs		B								B	
16. Magnetic tape (mini or cassette)											
17. Paper tape											
18. Punch cards											
19. Film											
20. Printer paper, carbon paper											
21. Printer ribbons											
22. Other ________________											

Case ID 7042

	a. Unauthorized removal	b. Unauthorized usage	c. Used in unintended ways	d. Unauthorized removal of a copy	e. Unauthorized modification	f. Total destruction	g. Reparable damage	h. Not achieved	i. Achieved partially	j. Achieved totally	k. Results unintended by suspects
3.3.3 Software											
22. Application programs											
23. System of application programs											
24. Library of application programs											
25. Job control instructions		B								B	
26. Operating system											
27. Supervisor											
28. Job scheduler											
29. Queueing control											
30. Interrupt processor		B								B	
31. Job swapper											
32. Resource allocation											
33. Storage manager											
34. I/O processors											
35. Operator control											
36. Accounting		B								B	
37. Recovery											
38. System initialization											
39. System bootstrap											
40. Library manager											
41. Job control translator											
42. Terminal manager											
43. Activity monitor											
44. Performance monitor											
45. Access controller											
46. Authorization controller											

Case ID 7042

	a. Unauthorized removal	b. Unauthorized usage	c. Used in unintended ways	d. Unauthorized removal of a copy	e. Unauthorized modification	f. Total destruction	g. Reparable damage	h. Not achieved	i. Achieved partially	j. Achieved totally	k. Results unintended by suspects
47. I/O drivers											
48. Compilers, assemblers, translators		B	B							B	
49. Utility programs		B	B							B	
50. Other ________________											
________________________											
3.3.4 Data											
51. Stored on-line application files				B						B	
52. Stored off-line application files											
53. Machine-readable input data											
54. Machine-readable output data											
55. Input data for conversion											
56. Output reports											
57. Operations records				B						B	
58. Active operating system tables,files				B						B	
59. Security authorization tables				B						B	
60. User identification tables				B						B	
61. System monitoring files				B						B	
62. Buffer files											
63. Queueing files											
64. Other ________________											
________________________											
3.3.5 Documents											
65. System software manuals		B								B	
66. System user manuals		B								B	

Case ID 7042

	a. Unauthorized removal	b. Unauthorized usage	c. Used in unintended ways	d. Unauthorized removal of a copy	e. Unauthorized modification	f. Total destruction	g. Reparable damage	h. Not achieved	i. Achieved partially	j. Achieved totally	k. Results unintended by suspects
67. System software specifications											
68. System design documents		C								C	
69. System usage aids		C								C	
70. System newsletters											
71. Maintenance documents		C								C	
72. Hardware manuals		C								C	
73. Hardware drawings											
74. Operator instructions											
75. System status reports											
76. Data control instructions											
77. Audit documents											
78. Security documents											
79. Data preparation instructions											
80. Application manuals											
81. Application specifications											
82. Organization procedures, charts											
83. Personnel lists											
84. Published reports, papers											
85. Unpublished reports, papers											
86. Other ____________											

3.3.6 Facilities

86. Doors											
87. Windows											
88. Walls											
89. Floors											

Case ID 7042

	a. Unauthorized removal	b. Unauthorized usage	c. Used in unintended ways	d. Unauthorized removal of a copy	e. Unauthorized modification	f. Total destruction	g. Reparable damage	h. Not achieved	i. Achieved partially	j. Achieved totally	k. Results unintended by suspects
90. Ceilings											
91. Locks											
92. Safety equipment											
93. Power supply											
94. Oral communication equipment											
95. Air conditioning equipment											
96. Lights											
97. Security alarms											
98. TV equipment											
99. Photographic equipment											
100. Furniture											
101. Furnishings											
102. Data keying devices											
103. Off-line processors											
104. Other ________________											
________________											

Case ID 7042

3.4 Actions taken by suspects to avoid detection (Insert capital letters to identify participants).

	Restore a.	Change b.	Destroy c.	Remove d.	Contributed to Detection e.
1. System logs					
2. Security log					
3. Program changes					
4. Data changes					
5. Label or name changes					
6. Programs					
7. Data					
8. Buffer contents					
9. Storage contents					
10. Fingerprints, pictures					
11. Waste materials					
12. Moved equipment					
13. Moved media					
14. Moved materials					
15. Telephone circuit usage log					A
16. Other ________					
17. ________					

3.4.1 Describe System crash disguised access. Telephone circuits were used for short periods to avoid tracing.

3.4.2 Detection. (Circle appropriate letters) a. Before acts could occur. [✓ b.] During acts. c. After acts, time period ________. d. Accidental discovery. [✓ e.] By established detection methods. [✓ f.] Suspects identified. [✓ g.] Suspects caught.

Case ID 7042

3.4.3 Participants in detection and suspect identification. (Use capital letters to identify participants.)

	a. Detection	b. Suspect Identification
1. Computer operations staff	A	A
2. Security staff		
3. Audit staff		
4. Systems programming staff		
5. Hardware maintenance staff		
6. Applications staff		
7. Janitorial staff		
8. Vendor's staff		
9. System users		
10. Customer support staff		
11. Other ______		

3.4.4 Describe detection Detection was made by telephone company which traced leased line calls.

3.5 Suspects' positions relative to the acts and systems involved. (Circle appropriate numbers and prefix capital letters to identify suspects.)

___1. Computer system management. A [✓ 2.] Company management. B [✓ 3.] Application programmer/analyst. ___4. System designer. C [✓ 5.] System programmer/analyst. ___6. Program maintenance. ___7. Auditor. ___8. Data clerk. ___9. Security guard. ___10. Building maintenance worker. ___11. Hardware maintenance engineer. ___12. Data conversion operator. ___13. Computer/peripheral operator. ___14. Courier or messenger. ___15. Outside consultant. ___16. Company employee (not in computer system staff). ___17. Vendor's employee, on-site. ___18. Vendor's employee, off-site. C [✓ 19.] Internal customer of system. B [✓ 20.] External customer of system. B [✓ 21.] Business competitor's employee. ___22. Business associate employee. ___23. A person involuntarily served or affected by the computer system. ___24. A person voluntarily served or affected by the computer system. ___25. Social or political dissident. ___26. Other ______. ___27. Other ______

Case ID 7042

3.5.1 Knowledge and experience of the suspects. (Identify each suspect by a capital letter. Multiple entries for a single box are acceptable.)

	a. Knowledge	b. Experience	c. Not authorized	d. Authorized	e. Of systems involved in these acts	f. Necessary to accomplish the acts	g. Faulty knowledge or error resulting in failure	h. Faulty knowledge or error resulting in detection
1. Access to facilities	C	C		C	C	C		
2. Operation of terminals	BC	BC		BC	BC	BC		
3. Operation of peripherals								
4. Operation of communications	C	C		C	C	C		
5. Operation of computer	C	C		C	C			
6. Job submission	BC	BC		BC	BC	BC		
7. Access identification	BC	BC		BC	BC	BC		
8. Data submission								
9. Data preparation								
10. Data conversion								
11. Data control								
12. Application program use	BC	BC		BC	BC	BC		
13. Application program modification	BC	BC	C	B	BC	BC		
14. Application programming	BC	BC		BC	BC	BC		
15. Systems programming	C	C		C	C	C		
16. Operating system modification	C	C		C	C	C		
17. Computer modification	–							
18. Peripherals modification								

	a. Knowledge	b. Experience	c. Not authorized	d. Authorized	e. Of systems involved in these acts	f. Necessary to accomplish the acts	g. Faulty knowledge or error resulting in failure	h. Faulty knowledge or error resulting in detection
19. Terminals modification								
20. Communication modification								
21. Wiretapping								
22. Radiation pickup								
23. System security modification								
24. System auditing								
25. System testing								
26. Acquainted with staff	C	C		C	C			
27. Acquainted with users/customers	C	C		C	C	C		
28. Organization procedures	C	C		C	C	C		
29. Staff working schedules	C	C		C	C			
30. System schedules	C	C		C	C	C		
31. Independent training course								
32. Internal training course								
33. Other ________________								

3.6 Estimate of value of losses, injuries and damages: $________________

3.7 Changes made in the computer system as a result of these acts. Security increased? yes [✓ no] DescribeThe lack of system protection from assigned GO TO's has not been made at A or at any other GE 400 commercial time-sharing service.

Case ID 7042

3.8 Most important implications of this case Ease of gaining knowledge, skill, access. Use of poor system design or poor implementation resulting in incomplete handling of illegal program practice.

3.9 Additional information A is being acquired by Rapidata, Fairfield, New Jersey.

COMPUTER-RELATED INCIDENT QUESTIONNAIRE

PART 4, SUSPECT INVESTIGATION (One form for each Suspect)

4.1 Interviews

Date	Interviewer	Interviewee	Location
11/27/72	D. B. Parker	B	By telephone

4.2 Background

4.2.1 Name B Age 21 Sex M

4.2.2 Home address

Telephone

4.2.3 Work address

Telephone

4.2.4 Education (Circle) High school 1 2 3 [✓ 4] years. Location

College 1 2 3 4 years. Locations

Degree	Subject	Institution	Year

Professional society membership

4.2.5 (Circle appropriate letters) a. Married b. Separated c. Divorced

d. Widowed e. Single Children: Age __ Age __ Age __ Age __

4.2.6 Present employer Another time-sharing firm Years

Occupation or title

Brief job description

4.2.7 Other business interests

4.2.8 Salary (Circle a letter) a. less than $6000 b. 6000-7999 c. 8000-9999

d. 10,000-13,999 e. 14,000-17,999 f. 18,000-23,999 g. 24,000-29,999

h. 30,000-39,999 h. 40,000-49,999 i. More than 50,000

4.2.9 Recent employment (Most recent first)

Employer	Position	From	To

4.2.10 Criminal history. Number of arrests 1 Number of convictions 0

Arrest Charges	Date	Disposition
Transmission of stolen properties interstate by wire	7/29/70	Charges dropped

4.3 Suspect's involvement in the incident.

B conspired with C to gain knowledge to penetrate the operating system in Master Mode from his terminal. He penetrated the system on numerous occasions taking system files, user files and crashing the system. It is suspected the acts were malicious mischief. He had been using the service legitimately as a high school student and was then employed by a competitor of A.

4.4 Before the acts

4.4.1 Purpose of the acts (Circle appropriate letters). a. Direct financial gain by acquiring a negotiable instrument or transfer of credit. b. Indirect financial gain by converting results of the acts to financial gain. c. Personal advancement. d. Revenge. e. To support ideals. f. To right a wrong. [✓ g.] A challenge. [✓ h.] Curiosity. [✓ i.] Self-amusement. j. Amusement of others. k. To help somebody else. l. Other

4.4.2 Source of the idea for perpetrating the acts. (Circle appropriate letters.) a. Accident or error demonstrated the possibilities. b. Learned of similar acts. c. Had performed imilar acts. [✓ d.] Associates or friends performed similar acts. e. Associates or friends talked about similar acts. [✓ f.] Exposure of the target represented a temptation. [✓ g.] Apparent ease of the acts represented a temptation. h. Other

4.4.3 Attitude of the suspect towards potential individual, personal victims, if any. (Circle appropriate letters) a. Sorry. b. Sympathetic. c. Hostile. d. Superior to them. e. Inferior to them. [✓ f.] Indifferent. g. Other

4.4.5 Other similar acts suspect was aware of.

Act	Source
Test penetration of the system by a systems programmer employee of A	C as described by A

4.4.6 Planning. (Circle appropriate letters) a. Acts were not planned. b. Acts were partially planned. [✓ c.] Acts were completely planned. d. Planning was a full time effort. [✓ e.] Planning was a part time effort. f. Cost of the acts was estimated. g. Risk was evaluated. h. Sanctions if caught were known. [✓ i.] Avoidance of discovery was planned. j. Discovery was expected after the acts were perpetrated. k. If caught, exposure to family, friends or associates was feared. l. If caught, public exposure was feared. [✓ m.] Certain of carrying out plans. n. Uncertain of carrying out plans. o. Would be successful even though caught or exposed. [✓ p.] Would not be successful if caught or exposed. [✓ q.] Confident of success. r. Not confident of success. [✓ s.] Was not aware of criminal nature of the acts. t. Was not aware of unethical, unfair or immoral nature of the acts. [✓ u.] A change in protection of the system could have aborted plans. [✓ v.] New knowledge required. w. New knowledge not required. x. New skills required. [✓ y.] New skills not required. [✓ z.] Planning included other participants. [✓ *] Act planned from a position of trust.

4.4.7 New skills acquired

4.4.8 New knowledge acquired Fortran weakness, interrupt specifications, Master Mode, operating system organization, use of leased telephone circuits.

4.4.9 Collusion (Place an asterisk before name of the planning leader if not the suspect)

Name	Relationship to Suspect	Nature of Involvement
* C	Friend	transfer of knowledge

4.4.10 Date act was first conceived

By whom

4.4.11 Planning period. From to

4.5 During the acts

4.5.1 Period of time to conduct the acts (date, time). From 5/28/70 to 6/23/70

4.5.2 Actions (Circle appropriate letters) a. Compulsive. b. Frightened. c. Confident. [✓ d.] Methodical. e. Disorganized. [✓ f.] Followed plans. g. Deviated from plans. h. Encountered unexpected situations. i. Aware of witnesses. j. Careful to remove evidence. k. Not concerned with evidence. [✓ l.] In collusion with others. m. No collusion. n. Required cooperation of innocent people. [✓ o.] No cooperation of others required. [✓ p.] Actions were against a system. q. Actions were against people. [✓ r.] Posed or disguised as somebody else. s. Acted under his own identity. t. Fearful of detection. u. Not fearful of detection. [✓ v.] Successful. w. Partially successful. x. Not successful.

4.5.3 Collusion in the acts (Place an asterisk before name of the leader if not the suspect)

Name	Relationship to Suspect	Nature of Involvement
C		

4.5.4 Witnesses

Name	Relationship to Suspect	Nature of Involvement
A's computer operator	none	observed crashes

4.5.5 Suspect disguised or posed as A's system programmer

4.5.6 Mistakes and deviation from plans Used the leased line long enough to be traced

4.5.7 Reasons for success or failure Successful because of detailed knowledge of the system

4.6 After the acts

4.6.1 (Circle appropriate letters) a. Eager to discuss his actions. b. Willing to discuss his actions. [✓ c.] Unwilling to supply information. [✓ d.] Left the scene of his actions normally. e. Left the scene in haste or abnormally.

f. Sees himself as a hero. g. Is remorseful. h. Is self-righteous. [✓ i.] Is indifferent. j. Is elated. k. Shows animosity toward victims. l. Shows animosity toward other involved parties. m. Believes his actions were appropriate for the circumstances. [✓ n.] Feels he was wrong in his actions. o. Would repeat the actions under similar circumstances. p. Would never repeat his actions. q. Willing to make restitution. r. Not willing to make restitution. s. Feels he made a net gain towards his objectives. t. Suffered a net loss towards his objectives.

4.6.2 What did the suspect fear most (Rank by numbers or leave blank if not applicable)

a. ___ Discovery of the act

b. ___ Exposure of him as the perpetrator

c. ___ Harm to others

d. ___ Punishment

e. ___ Publicity

f. ___ Other ______________________

g. ___ Other ______________________

4.6.3 Feelings towards other involved parties

Name	Feelings

4.6.4 What circumstances would have stopped the suspect's actions? His awareness of detection

4.6.5 Alternative actions suspect could have taken:

Action	Reason for Rejection
Financial gain from his acts	