FDLE

Florida Department of Law Enforcement

COMPUTER CRIME IN FLORIDA 1989

12-4-90

MFI

124840

124840

James T. Moore, Commissioner

Honorable Bob Martinez, *Governor*
Honorable Jim Smith, *Secretary of State*
Honorable Bob Butterworth, *Attorney General*
Honorable Gerald Lewis, *Comptroller*
Honorable Tom Gallagher, *Treasurer*
Honorable Doyle Conner, *Commissioner of Agriculture*
Honorable Betty Castor, *Commissioner of Education*

James T. Moore, Commissioner
Florida Department of Law Enforcement

PREFACE

This report has been prepared by the Florida Department of Law Enforcement as part of our continuing goal of assessing changing crime problems and trends in the State of Florida. This identification process often involves conducting studies and strategic assessments in an effort to fully determine the extent of the problem. Emphasis is placed on those problem areas which exhibit a potential for increased criminal activity and which may adversely impact law enforcement resources. As a result of this effort, law enforcement at all levels will become more informed on emerging or changing crime trends so appropriate responses and actions can be formulated.

It is in keeping with this goal that the report "Computer Crime in Florida", has been prepared.

For additional information, questions or comments concerning this report, please contact the Florida Department of Law Enforcement, P.O. Box 1489, Tallahassee, Florida, 32302, Attention: Investigative Analysis Bureau, or call (904) 488-0586, SunCom 278-0586.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

This comprehensive research project could not have been successfully completed without immeasurable assistance from the following:

Mr. Francis "Buzz" Bruno, Principal, The Spinnaker Group Consultants, Tampa, Florida

The Florida State University Computer Center, Tallahassee, Florida

The American Bar Association, Section of Criminal Justice, Washington, D.C.

I would like to especially thank the many people from the law enforcement agencies, State Attorney's Offices and other public and private organizations who took time out of their busy schedules to respond to this survey.

Jeffery A. Herig
Special Agent
Florida Department of Law Enforcement

INTRODUCTION

Since the invention of computers roughly 40 years ago, the computer industry has experienced tremendous growth. Currently ranked as the third largest industry in the world, computers are firmly established as tools of everyday living. The introduction and subsequent widespread use of personal computers (PC's), is responsible for much of the growth in the industry. With the advent of the PC, computer technology has been placed in the hands of millions of Americans who are eager to utilize the capabilities of computers in business, science, education and the home. The proliferation of computers has brought about an unfortunate but predictable side effect: computer-related crimes. Consider the following examples:

- A federal employee in South Florida was charged with unauthorized entry into a computer after it was discovered he had directed a Customs Service computer to write more than $160,000 in fraudulent government checks to himself and three other subjects.

- An employee of a Central Florida financial institution was arrested after it was discovered he had used a company computer to divert $280,000 from customers' accounts to his own account.

- A teenager in North Florida was charged with gaining unauthorized access to a Florida Department of Education computer system. He had been trying to gain access to the system for weeks using a personal computer at his home.

Incidents such as these begin to illustrate the seriousness of computer-related crime and remove any notion that these are "victimless" crimes perpetrated by misguided individuals. The fact is, computer-related crimes can involve substantial monetary losses as well as countless hours of lost productivity to public organizations and private businesses. Computer-related crimes can vary from relatively simple schemes to very complex and technically sophisticated crimes.

Although it is difficult to precisely define computer crime, a working definition had to be developed. For purposes of this study, computer crime has been defined as any crime in which the computer is either the tool of the crime or where it is the object of the crime. This can include both traditional crimes as well as newly emerging and highly sophisticated crimes in which a computer is used.

Law enforcement agencies in Florida are now confronted with this technology as more incidents of crimes involving computers are reported. The primary purpose of this study was to determine the extent of computer crime in Florida and to assess what impact it may be having on local law enforcement agencies and prosecutors in the State. This was accomplished through the use of a survey questionnaire which was sent to businesses, law enforcement agencies and prosecutors in Florida. This is the first study which looks at the computer crime problem in Florida. It is hoped that information contained in this document will assist local law enforcement agencies in their efforts to recognize and address the problem of computer-related crime in Florida.

EXECUTIVE SUMMARY

METHODOLOGY

The study consisted of developing three different survey questionnaires on the topic of computer crime which were sent to three different survey groups. The three groups consisted of:

1. 382 Sheriff's, Police and Public Safety Departments in Florida.
2. 20 State Attorney's Offices in Florida.
3. 898 public and private sector organizations in Florida.

The 898 organizations surveyed consisted of organizations who had computer systems currently in operation at their facilities. Systems ranged from microcomputers to large system mainframes. Included in this group were public and private organizations from manufacturing, universities, defense industry, service industries and governmental agencies etc. In order to obtain a representative sample of businesses from all counties in Florida, a formula of selecting one (1) business per 40,000 county population was used with a minimum of 2 businesses per county for those counties with less than 40,000 population.

A total of 702 responses were received for an overall return rate of 54%. The response by group was as follows:

1.	Law Enforcement:	281	returned	73.6%
2.	State Attorneys:	18	returned	90.0%
3.	Businesses:	403	returned	44.9%

HIGHLIGHTS

A number of significant findings were revealed from the responses. Following is a synopsis of the major findings:

- 1 out of 4 business respondents reported they were a victim of some type of computer crime in the last 12 months. The types of crimes committed were most often theft of computer hardware and software, unauthorized use of computer resources and destruction or alteration of computer software and data.

- Law enforcement agencies in Florida have only been exposed to a limited amount of computer crime investigations. Sixty-seven (67) agencies reported that they had investigated from 1-10 computer crimes in the last 12 months. Only 20 agencies indicated they had investigated more than 10 computer crimes in the last 12 months.

- State Attorney's Offices have also been exposed to only a limited amount of computer crime. Twelve (12) of the eighteen (18) State Attorney circuits responding indicated they had received for prosecution from 1-10 computer crime-related cases in the last 12 months, 3 had received more than 10 cases and 3 circuits reported they had received no computer crime cases for prosecution.

- Monetary losses to organizations due to computer crime were reported as high as $1 million in the last 12 months. However, most organizations reported they either had no estimate of losses or no available system to monitor losses.

- All three survey groups reported that computer crime suspects, when identified, were most often employees of the victim organization.

- 28 organizations reported they suspect or are convinced there is computer crime currently occurring in their organizations.

- Based on their experience, business respondents did not rate highly the effectiveness of federal, state and local law enforcement agencies in computer crime investigations.

- All three survey groups felt computer criminals were motivated most by the lure of personal financial gain and second by the intellectual challenge.

- Training for law enforcement in computer crime investigations is almost nonexistent. Eighty percent (80%) of the law enforcement respondents reported adequate training in computer crime investigations is not available. Further, 85% of the respondents also reported they had no sworn personnel with any training in computer crime investigations. Eighty percent (80%) of the State Attorney respondents felt the law enforcement agencies in their respective circuits did not have adequately trained personnel in computer crime investigations.

- According to the respondents in all three groups, the best improvements that can be made in combatting computer crime include better self-protection by organizations, better training for law enforcement in computer crime investigations and better methods for detecting computer crime.

SURVEY RESULTS AND ANALYSIS

SURVEY RESPONSE

All three survey groups enthusiastically responded to the survey questionnaire. The high response rates were clearly indicative of a keen interest and deep concern in the area of computer crime by all three groups. Figure 1 depicts the breakdown of the response rates for each of the three groups:

Figure 1

	MAILED	RETURNED	PERCENT
Law Enforcement:	382	281	73.6%
State Attorneys:	20	18	90.0%
Businesses:	898	403	44.9%
Overall Response Rate:	1300	702	54.0%

ABOUT THE RESPONDENT GROUPS

Each of the respondent groups was asked a few questions which dealt with size, population, revenues, etc. The answers to these questions provide an overview of the types of organizations that responded to the survey.

Almost half of the law enforcement agencies responding (47.5%), had a jurisdiction size of less than 10,000 people. Sixty-three percent (63%) of the agencies had less than 50 total employees in their respective agencies. By far the majority of law enforcement agencies in Florida are relatively small and have only limited resources. The large metropolitan agencies with hundreds of personnel and more extensive resources are the exception.

Of the 18 State Attorney respondents, almost half (8), had a circuit population size of between 100,000 and 500,000. Eight (8) respondents indicated there were over 50 attorneys employed in their offices.

The business survey respondents were engaged in many different types of business. A significant number were from Manufacturing, Medical Services, Federal, State and Local Government, Computers and Electronics, and Banking and Financial Services. The annual revenues or budgets of the businesses were reported as high as over $1 billion. Of the 308 respondents to the question, 107 (28.2%) reported an annual budget or revenues of between $10 million and $50 million. The number of employees in the organizations ranged from under 100 (161 responses) to as high as between 50,000 and 100,000 (1 response).

Over 85% of the business respondents were either executives, supervisors or managers with direct responsibility over computers, their operation and/or their security. The validity of this study is enhanced by the fact that such a large majority of respondents were directly involved with their organization's computer operations and security.

INCIDENTS OF COMPUTER CRIME

Each of the survey groups was asked a number of questions in reference to incidents of computer crime they either experienced, investigated or prosecuted, depending on the particular survey group. A significant number of revealing results emerged which are explained in this section.

The business survey asked respondents to indicate the types of known and verifiable incidents of computer crime they may have experienced in the last 12 months. Of the 393 respondents that answered this question, 24.2% (95) indicated they had experienced some type of known and verifiable computer crime in the last 12 months. This translates to 1 in 4 businesses surveyed being a victim of computer crime in the last 12 months. The most prevalent types of computer crime experienced were:

- Theft of computer hardware and software
- Unauthorized use of computer resources
- Destruction or alteration of computer software and computer data

Known and verifiable monetary losses due to computer crime were reported by 20.8% (82) of the business respondents. Losses ranged from less than $10,000 to as high as $1 million. The majority of respondents however, indicated they either had no system to monitor losses or no estimated value of losses.

The law enforcement respondents were asked how many cases of computer crime they investigated in the last 12 months. Over 2 out of 3 agencies (193), had not investigated any cases of computer crime in the last 12 months. Another 23.9% (67), of the agencies had investigated from 1-10 crimes.

The law enforcement respondents were also asked to indicate the types of computer crimes they had investigated. The major types of crimes investigated in order of frequency were:

- Theft of computer hardware and software
- Theft of tangible or intangible assets involving a computer
- Embezzlement involving a computer
- Fraud involving a computer

These results indicate that computer crime involves both instances where the computer is the object of the crime, and where it is the tool of the crime.

The State Attorneys were asked how many cases of computer crime they had received for prosecution in the last 12 months. Of the 18 responses, 12 indicated they had received from 1 to 10 cases; 2 reported they received between 11 and 25 cases and one circuit reported receiving as high as between 26 and 50 cases in the last 12 months.

It should be noted that not all cases reported to law enforcement are forwarded to the State Attorney for prosecution. In many cases, no suspect is identified or arrested, precluding the need for any further action in the case. This may explain why the law enforcement respondents reported more cases of computer crime than the State Attorneys had reported.

Both the law enforcement and State Attorney surveys asked the respondents if they thought computer crime was increasing, decreasing or staying the same in their respective jurisdictions. Figure 2 below depicts the results.

Figure 2

	Law Enforcement Responses	State Attorneys Responses
Increasing	36	8
Decreasing	2	0
Staying the Same	80	5
Unknown	151	5
	269	18

Finally, the business respondents were asked whether they thought there was computer crime currently occurring in their organizations, regardless of whether they had previously been a computer crime victim. Twenty-eight (28),organizations reported they suspect or are convinced there is computer crime occurring in their businesses at this time.

REPORTING COMPUTER CRIME

The law enforcement and State Attorney respondents were asked their opinions on how often they believe incidents of computer crime were reported. The business respondents were similarly asked how often they actually report incidents of computer crime. The results are shown in Figure 3.

Figure 3

	Law Enforcement (Opinion)	State Attorneys (Opinion)	Businesses (Actual)
All Incidents Reported:	3%	0%	24%
Most Incidents Reported:	9	0	1
Some Incidents Reported:	83	94	9
No Incidents Reported:	5	6	65

As shown above, 65% of the organizations surveyed reported they did not report to law enforcement authorities any incidents of computer crime they experienced. One of the questions this statistic raises is whether computer crime is not reported based on a perceived inability of law enforcement to effectively investigate computer crime or if organizations prefer not to disclose incidents of computer crime because of potentially adverse publicity and instead prefer to handle cases internally. The following analysis reveals at least part of the answer.

The business respondents were asked to rate the ability of law enforcement authorities to effectively investigate computer crime based on the previous experience of the respondent. They were asked to separately rate the federal, state and local law enforcement levels and were given the following four choices: Excellent, Good, Fair and Poor. Figure 4 depicts the compiled results of this question.

Figure 4

Federal Law Enforcement:	Fair to Good
State Law Enforcement:	Fair
Local Law Enforcement:	Poor

Although this may not be an overwhelming vote of confidence for law enforcement in computer crime investigations, it does serve to highlight the concern that law enforcement may not be adequately prepared to confront this emerging crime category.

As for the cases that have been reported to local law enforcement agencies, the law enforcement respondents were asked to indicate how computer crime cases are handled within their respective departments. Of the 92 responses that were applicable, 64.1% (59) reported that cases are assigned to "in-house" investigators using a standard case rotational method. Another 20.7% (19), indicated cases they received are assigned to an "in-house" investigator who has special knowledge or expertise in computer crime investigations. Two of the agencies reported they refer case(s) to other law enforcement agencies.

PERPETRATORS OF COMPUTER CRIME

Each of the survey groups was asked two similar questions regarding computer crime perpetrators.

The law enforcement respondents were asked to indicate who the computer crime perpetrators were when they were identified. In 50% of the cases reported to law enforcement where a suspect was identified, an employee within the victim organization was responsible for the crime. In another 19% of the cases, the perpetrator was identified as an individual outside of the victim organization, commonly known as a "hacker", gaining unauthorized access to the victim's computer system.

The State Attorney respondents also cited employees of the victim organization as the most likely perpetrators of computer crimes in cases where a suspect was identified.

The business respondents were asked to provide information about computer crime perpetrators in reference to incidents that occurred in their organizations. In cases where a suspect was identified, 84% were employees within the victim organization.

All three survey groups were also asked what they felt motivated computer crime perpetrators. The vast majority of respondents in all three groups felt computer criminals were most often motivated by personal financial gain. Other motivators often listed were, in order:

- The intellectual challenge
- Corporate financial gain
- Other personal reasons

COMPUTER CRIME TRAINING

This section addresses the issue of computer crime training for both the law enforcement and State Attorney survey groups.

The law enforcement respondents were asked whether any members of their respective agencies have attended any seminars, courses and/or workshops on the topic of computer crime investigations. Of the 278 responses to this question, 85.3% (237) stated they have no personnel who have attended any seminars, courses or workshops on the topic of computer crime investigations.

The agencies that did indicate they had personnel with some training were then asked to indicate how many sworn employees have attended at least one seminar, course or workshop on computer crime investigations. Most of the 41 agencies reported they either had one or two employees who have attended training. The law enforcement respondents were asked whether they feel adequate training is currently available to law enforcement agencies in computer crime investigations. Of the 235 responses, 80% (188), felt adequate training is not available for law enforcement agencies in computer crime investigations.

The State Attorney respondents were asked whether they felt the law enforcement personnel in their respective jurisdictions had adequately trained personnel in computer crime investigations. Of the 17 responses, 16 indicated they did not feel law enforcement agencies had adequately trained personnel.

Relating to this issue, the State Attorney respondents were asked to indicate some of the problems they may be encountering in the prosecution of computer crime cases. The three most often indicated areas of concern in order of importance were:

- A general lack of available training, literature or information for prosecutors in the area of computer crime

- Improper or inadequate case development or handling by law enforcement

- Difficulty in juries understanding technical aspects of computer crime

IMPROVEMENTS IN COMBATTING COMPUTER CRIME

Respondents of all three surveys were asked to rank in order, six given choices of improvements that could be made in combatting computer crime. They were asked to order their responses in descending or priority order. Following is the compiled rankings for each of the survey groups:

Law Enforcement	State Attorneys	Businesses	
1	2	1	More comprehensive and effective self-protection by private business.
3	3	2	Better methods for detecting computer crime.
5	5	6	Better education of the general public regarding computer crime.
2	1	4	Better training for law enforcement in computer crime investigations.
4	4	3	Increased prosecution of perpetrators when identified.
6	6	5	More severe criminal penalties for computer crime perpetrators.

The law enforcement and State Attorney respondents ranked the choices almost identically. In the two categories they did not, the choices were reversed. All three groups felt better self-protection, (prevention of computer crimes) was one of the best improvements that could be made. Better training for law enforcement was seen by law enforcement and State Attorneys as a very high priority in combatting computer crime. The least important improvement of the choices given was more severe penalties for computer crime perpetrators.

The responses to this question convey an attitude by the respondents that efforts should be concentrated on preventing computer crime rather than depending on the possibility of stiff criminal penalties to deter potential criminals.

SURVEY COMMENTS

At the conclusion of each survey, the respondents were asked to provide any additional comments they wished to make in reference to the study. Following are a few selected additional comments from the returned surveys:

From Businesses:

- "Glad to see statewide attention on this issue".

- "As consultants, our firm has been contacted several times during the past year regarding various computer crimes".

- "The use of encryption techniques can help protect sensitive data. Software protection schemes for PC's is more of a challenge than a protection".

From Law Enforcement:

- "Thorough training, both technical and legal, are almost totally lacking, both for the business and police communities, in terms of preventing, detecting and prosecuting computer-related offenses".

- "An FDLE course on computer crime would be appropriate".

- "Incidents of computer offenses reported to this agency have primarily involved fraud or theft of services via computer from long distance telephone services".

From State Attorneys:

- "The computer crime cases that have been brought to this office have not been particularly complex. Therefore, it is unknown whether law enforcement agencies have adequately trained personnel".

RECOMMENDATIONS

The results of this study clearly illustrate that computer-related crime is a reality in Florida today. As evident in this study, computer crime is not the exclusive problem of either the private sector or the law enforcement community. The question is then, what can be done to enhance efforts to prevent incidents of computer crime and to investigate and prosecute reported cases? Following are a number of recommendations that address some possible solutions:

- Organizations that utilize computers for information processing need to implement adequate controls to both prevent incidents of computer crime and to provide a system for monitoring security breaches and losses in the event an incident occurs. These controls must recognize the fact that employees are more likely perpetrators than outsiders.

- Law enforcement agencies must critically evaluate their current capabilities to investigate computer-related crimes. The most effective initial step an agency can take to improve their capabilities is to sponsor enrollment of their members in basic microcomputer operations and familiarity courses. Although these are not law enforcement oriented investigative courses, they are an important first step in overcoming any apprehension of computers. These courses are often short in duration and are offered in most communities by computer retailers, technical centers, adult education programs and community colleges. Some members will find that after taking an introductory course, they develop a further interest that leads to advanced learning.

- Training must be developed and provided for law enforcement in specific computer crime investigative techniques. Beyond basic familiarity courses, there is a distinct void in law enforcement training oriented to computer crime investigations.

- Prosecutors must work to educate themselves on the many complex aspects of computer crime litigation. This process begins with basic computer operations and familiarity courses offered in the community as mentioned above. Prosecutors are presented with the difficult task of having to educate judges and juries on technical aspects of cases they may not fully understand themselves.

One positive step already taken in the fight against computer crime has been the enacting of a state statute. Florida was one of the first states to pass a comprehensive computer crime law. Florida State Statute 815, known as the Florida Computer Crimes Act, is an effective tool that must be increasingly utilized by the criminal justice system. Only through increased awareness and action can the private sector and the criminal justice community meet the challenge of effectively combatting computer-related crime.

APPENDIX A

LAW ENFORCEMENT QUESTIONNAIRE

1. My agency's jurisdiction has a population size of:

	Responses	Percent
Less than 10,000	132	47.5%
Between 10,001 and 50,000	95	34.2
Between 50,001 and 100,000	23	8.3
Between 100,001 and 500,000	24	8.6
Between 500,001 and 1 million	2	.7
Over 1 million	2	.7
Total Responses	278	100.0%

2. The total number of employees in my agency including sworn and non-sworn personnel is:

	Responses	Percent
Less than 50	177	63.2%
Between 51 and 100	38	13.6
Between 101 and 500	53	18.9
Between 501 and 1000	8	2.9
Over 1000	4	.4
Total Responses	280	100.0%

3. In the last 12 months, my agency has investigated the following number of computer-related crimes:

	Responses	Percent
None	193	68.9%
Between 1 and 10	67	23.9
Between 11 and 25	15	5.4
Between 26 and 50	3	1.1
Between 51 and 100	1	.4
Over 100	1	.4
Total Responses	280	100.1%

4. Overall, it appears to me that the total number of computer-related crimes in my jurisdiction is:

	Responses	Percent
Increasing	36	13.4%
Decreasing	2	.7
Staying about the same	80	29.7
Unknown	151	56.1
Total Responses	269	99.9%

5. My agency has investigated the following types of computer-related crimes: (multiple answers allowed)

	Responses	Percent
Not Applicable	185	39.4%
Destruction or alteration of computer hardware	10	2.1
Destruction or alteration of computer software	10	2.1
Destruction or alteration of data	16	3.4
Theft of computer hardware	71	15.1
Theft of computer software	39	8.3
Theft of input data	11	2.3
Theft of raw output data	13	2.8
Theft of coded output data	9	1.9
Theft of assets, tangible or intangible, involving a computer	31	6.6
Fraud involving a computer	24	5.1
Extortion/Blackmail involving a computer	5	1.1
Embezzlement involving a computer	27	5.7
Sabotage involving a computer	3	.6
Unauthorized use of computer resources for personnal programming activities	7	1.5
Other	9	1.9
Total Responses	470	99.9%

Significant "Other" comments:

-Use of computer in traditional type crimes, i.e., pornography, narcotics
-ATM crimes

6. With respect to the incidents of computer crime that my agency has investigated, the perpetrators have been: (multiple answers allowed)

	Responses	Percent
Not Applicable	188	55.1%
Not identified	44	12.9
Non-data processing managers or supervisors within the victim org.	14	4.1
Other non-data processing employees within the victim organization	10	2.9
Data processing managers or supervisors within the victim organization	7	2.1
Other data processing employees within the victim organization	26	7.6
Competitors of victim organization	11	3.2
Individuals using personal computer to gain unauthorized access to another computer (hacker type incident)	21	6.2
Other	20	5.9
Total Responses	341	100.0%

Significant "Other" comments:

-Consultants hired by victim organization
-Common thieves and burglars

7. In my opinion, perpetrators of computer crime are motivated by: (multiple answers allowed)

	Responses	Percent
Personal financial gain	200	50.6%
Organizational/corporate financial gain	49	12.4
Organizational/peer group pressure	23	5.8
The intellectual challenge	64	16.2
Other personal reasons	33	8.4
Other	26	6.6
Total Responses	395	100.0%

Significant "Other" comments:

-Narcotics dependency
-Revenge

8. Most incidents of computer crime reported to my agency are:

	Responses	Percent
Not applicable	179	66.1%
Referred to another law enforcement agency	2	.7
Assigned to an in-house investigator with special knowledge or expertise in computer crime investigations	19	7.0
Assigned to an in-house investigator using standard rotation procedure	59	21.8
Other	12	4.4
Total Responses	271	100.0

Significant "Other" comments:

-Worked in-house with outside expert assistance

9. In my opinion, the best improvements that can be made in combatting computer crime are: (rank order 1-7 with 1 being the best improvement)

	Compiled Rankings
More comprehensive and effective self-protection by private business	1
Better methods for detecting computer crime	3
Better education of the general public regarding computer crime	5
Better training for law enforcement in computer crime investigations	2
Increased prosecution of perpetrators when identified	4
More severe criminal penalties for computer crime perpetrators	6
Other	7

Question 9 continued...

Significant "Other" comments:

-Better training for prosecutors
-Better user security awareness
-Second set of serial numbers inside computer

10. With respect to the incidents of computer-related crime in the private sector, I believe:

	Responses	Percent
All such incidents are reported to law enforcement	8	3.4%
Most incidents are reported to law enforcement	20	8.5
Some incidents are reported to law enforcement	195	82.6
None of the incidents are reported to law enforcement	13	5.5
Total Responses	236	100.0%

11. Sworn member(s) of my agency have attended seminar(s), course(s) and/or workshop(s) on the topic of computer crime investigations:

	Responses	Percent
Yes	41	14.7%
No	237	85.3
Total Responses	278	100.0%

11a. If Yes, how many sworn employees have attended at least one seminar, course or workshop:

Total number of sworn employees: 68

12. Adequate training is currently available to law enforcement agencies in the area of computer crime investigations:

	Responses	Percent
Agree	47	20.0%
Disagree	188	80.0
Total Responses	235	100.0%

APPENDIX B

STATE ATTORNEY QUESTIONNAIRE

1. My Circuit has a population size of:

	Responses	Percent
Less than 10,000	0	0%
Between 10,001 and 50,000	0	0
Between 50,001 and 100,000	1	5.6
Between 100,001 and 500,000	8	44.4
Between 500,001 and 1 million	6	33.3
Over 1 million	3	16.7
Total Responses	18	100.0%

2. The total number of attorneys in my agency is:

	Responses	Percent
Less than 5	0	0%
Between 5 and 10	1	5.6
Between 11 and 20	3	16.7
Between 21 and 50	6	33.3
Over 50	8	44.4
Total Responses	18	100.0%

3. In the last 12 months, my agency has received, investigated, filed, and/or prosecuted the following number of computer-related crimes:

	Responses	Percent
None	3	16.7%
Between 1 and 10	12	66.7
Between 11 and 25	2	11.1
Between 26 and 50	1	5.6
Between 51 and 100	0	0.0
Over 100	0	0.0
Total Responses	18	100.1%

4. Of the total number of computer-related crime cases indicated in Question 3 above, the percentage that have been filed under F.S.S. 815, known as the Florida Computer Crimes Act, was:

	Responses
0	4
10 percent	2
20 percent	0
30 percent	1
40 percent	0
50 percent	1
60 percent	0
70 percent	0
80 percent	2
90 percent	1
100 percent	1
Total Responses	12

5. Overall, it appears to me that the total number of computer-related crimes in my Circuit is:

	Responses	Percent
Increasing	8	44.4%
Decreasing	0	0.0
Staying about the same	5	27.8
Unknown	5	27.8
Total Responses	18	100.0%

6. My agency has received, investigated, filed and/or prosecuted the following types of computer-related crimes:(multiple answers allowed)

	Responses	Percent
Not Applicable	3	4.6%
Destruction or alteration of computer hardware	1	1.5
Destruction or alteration of computer software	4	6.2
Destruction or alteration of data	7	10.8
Theft of computer hardware	3	4.6
Theft of computer software	5	7.7
Theft of input data	5	7.7
Theft of raw output data	1	1.5
Theft of coded output data	3	4.6
Theft of assets, tangible or intangible, involving a computer	9	13.8
Fraud involving a computer	6	9.2
Extortion/Blackmail involving a computer	3	4.6
Embezzlement involving a computer	6	9.2
Sabotage involving a computer	5	7.7
Unauthorized use of computer resources for personal programming activities	2	3.1
Other	2	3.1
Total Responses	65	99.9%

7. With respect to the incidents of computer-related crime in the private sector, I believe:

	Responses	Percent
All such incidents are reported to law enforcement	0	0.0%
Most incidents are reported to law enforcement	0	0.0
Some incidents are reported to law enforcement	16	94.1
None of the incidents are reported to law enforcement	1	5.9
Total Responses	17	100.0%

8. In my opinion, perpetrators of computer crime are motivated by: (multiple answers allowed)

	Responses	Percent
Personal financial gain	17	45.9%
Organizational/corporate financial gain	4	10.8
Organizational/peer group pressure	1	2.7
The intellectual challenge	7	18.9
Other personal reasons	6	16.2
Other	2	5.4
Total Responses	37	99.9%

Significant "Other" comments:

-Revenge

9. With respect to the incidents of computer crime that my agency has received, the suspects/perpetrators have been: (multiple answers allowed)

	Responses	Percent
Not Applicable	4	13.3%
Not identified	1	3.3
Non-data processing managers or supervisors within the victim org.	5	16.7
Other non-data processing employees within the victim organization	4	13.3
Data processing managers or supervisors within the victim organization	4	13.3
Other data processing employees within the victim organization	6	20.0
Competitors of victim organization	1	3.3
Individuals using personal computer to gain unauthorized access to another computer (hacker type incident)	5	16.7
Other	0	0.0
Total Responses	30	99.9%

10. In my opinion, the best improvements that can be made in combatting computer crime are: (rank order 1-7 with 1 being the best improvement)

	Compiled Rankings
More comprehensive and effective self-protection by private business	2
Better methods for detecting computer crime	3
Better education of the general public regarding computer crime	5
Better training for law enforcement in computer crime investigations	1
Increased prosecution of perpetrators when identified	4
More severe criminal penalties for computer crime perpetrators	6
Other	7

Significant "Other" comments:

-Better cooperation from victim organization in pursuing computer crimes from within their organizations.

11. As I see it, some of the problems confronting prosecutors in dealing with incidents of computer crime are: (multiple answers allowed)

	Responses	Percent
A less than adequately informed judiciary in regard to the nature of computer crime and computer crime offenders	7	14.6%
A general lack of available training/literature/information for prosecutors in the area of computer crime	13	27.1
Improper or inadequate case development or handling by law enforcement	12	25.0
Difficulty in juries understanding technical aspects of computer crime	10	20.8
Insufficient staff within the State Attorney's Office	5	10.4
Other	1	2.1
Total Responses	48	100.0%

12. In my opinion, law enforcement agencies in my Circuit have adequately trained personnel in the area of computer crime investigations:

	Responses	Percent
Agree	1	5.9%
Disagree	16	94.1
Total Responses	17	100.0%

APPENDIX C

BUSINESS QUESTIONNAIRE

1. My organization is engaged in the following type of business:

	Responses	Percent
Banking/Financial Services	20	5.4%
Insurance	8	2.1
Energy Production	4	1.1
Transportation	9	2.4
Manufacturing	69	18.5
Computers/Electronics	24	6.4
Communications	11	2.9
Legal Services	6	1.6
Construction	16	4.3
Medical Services	30	8.0
Federal Government	4	1.1
State Government	11	2.9
Local Government	34	9.1
Conglomerate	5	1.3
Other	122	32.7
Total Responses	373	99.8%

2. The annual gross revenue (or budget) of my organization is:

	Responses	Percent
Under $100,000	10	2.6%
Between $100,000 and $500,000	30	7.9
Between $500,000 and $1 million	28	7.4
Between $1 million and $5 million	77	20.3
Between $5 million and $10 million	42	11.1
Between $10 million and $50 million	107	28.2
Between $50 million and $100 million	40	10.5
Between $100 million and $500 million	36	9.5
Between $500 million and $1 billion	5	1.3
Over $1 billion	5	1.3
Total Responses	380	100.1%

3. The number of employees in my organization is:

	Responses	Percent
Under 100	161	40.0%
Between 100 and 1000	171	42.4
Between 1001 and 10,000	65	16.1
Between 10,001 and 50,000	5	1.2
Between 50,001 and 100,000	1	.2
Between 100,001 and 500,000	0	0
Over 500,000	0	0
Total Responses	403	99.9%

4. My involvement with computers and computer operations is:

	Responses	Percent
No involvement with computers	4	1.0%
As an executive with some responsibility/ oversight over computers, their operation or their security	100	25.1
As a supervisor or manager with direct responsibility/oversight over computers, their operation, or security	241	60.4
As a computer programmer, operator or system administrator	25	6.3
As a user of computers or computer services	9	2.3
As a manufacturer or retailer of computer hardware or software	10	2.5
Other	9	2.3
Total Responses	399	99.9%

5. My organization has experienced known and verifiable losses due to computer crime during the last 12 months of:

	Responses	Percent
Not applicable	313	79.2%
Up to $10,000	14	3.5
Between $10,000 and $50,000	8	2.0
Between $50,000 and $100,000	0	0.0
Between $100,000 and $500,000	0	0.0
Between $500,000 and $1 million	2	0.5
Between $1 million and $5 million	0	0.0
Between $5 million and $10 million	0	0.0
Between $10 million and $50 million	0	0.0
Between $50 million and $100 million	0	0.0
Over $100 million	0	0.0
No available system to monitor losses	38	9.6
No available estimate of value of losses	20	5.1
Total Responses	395	99.9%

6. My organization has experienced known and verifiable incidents involving the following types of computer crime: (multiple answers allowed)

	Responses	Percent
Not Applicable	298	63.7%
Destruction or alteration of computer hardware	10	2.1
Destruction or alteration of computer software	16	3.4
Destruction or alteration of data	16	3.4
Theft of computer hardware	29	6.2
Theft of computer software	21	4.5
Theft of input data	1	.2
Theft of raw output data	5	1.1
Theft of coded output data	1	.2
Theft of assets, tangible or intangible, involving a computer	10	2.1
Fraud involving a computer	2	.4
Extortion/Blackmail involving a computer	1	.2
Embezzlement involving a computer	9	1.9
Sabotage involving a computer	6	1.3
Unauthorized use of computer resources for personnal programming activities	30	6.4
Other	13	2.8
Total Responses	468	99.9%

Significant "Other" comments:

-Illegal use of passwords
-Improper use (games-lost work hours)
-Unauthorized external access

7. Whether or not my organization has been a victim of computer crime:

	Responses	Percent
I suspect or am convinced there is undetected computer crime currently occurring in my organization	28	7.0%
I do not believe there is undetected computer crime cuurrently occurring in my organization	394	93.0
Total Responses	402	100.0%

8. With respect to the incidents of computer crime that my organization has experienced, the perpetrators/suspects have been: (multiple answers allowed)

	Responses	Percent
Not Applicable	314	74.1%
Not identified	29	6.8
Non-data processing managers or supervisors within the victim org.	18	4.2
Other non-data processing employees within the victim organization	19	4.5
Data processing managers or supervisors within the victim organization	14	3.3
Other data processing employees within the victim organization	17	4.0
Individuals using personal computer to gain unauthorized access to another computer (hacker type incident)	5	1.2
Other	8	1.9
Total Responses	424	100.0%

Significant "Other" comments:

-Former employees
-Data Processing consultants

9. With respect to the incidents of computer-related crime that my organization experienced:

	Responses	Percent
Not applicable	320	80.4%
All such incidents were reported to law enforcement	19	4.8
Most incidents were reported to law enforcement	1	.3
Some incidents were reported to law enforcement	7	1.8
None of the incidents were reported to law enforcement	51	12.8
Total Responses	398	100.1%

10. Based on my experience, I would rate the ability of law enforcement to investigate computer crime as follows:

The choices were: Excellent, Good, Fair, Poor

	Overall Compiled Responses
Federal law enforcement	Fair to Good
State law enforcement	Fair
Local law enforcement	Poor

11. In my opinion, those that commit computer crime are motivated by: (multiple answers allowed)

	Responses	Percent
Personal financial gain	319	43.1%
Organizational/corporate financial gain	69	9.3
Organizational/peer group pressure	36	4.9
The intellectual challenge	196	26.5
Other personal reasons	98	13.2
Other	22	3.0
Total Responses	740	100.0%

Significant "Other" comments:

-Revenge
-Prove power

12. In my opinion, the best improvements that can be made in combatting computer crime are: (rank order 1-6 with 1 being the best improvement)

	Compiled Rankings
More comprehensive and effective self-protection by private business	1
Better methods for detecting computer crime	2
Better education of the general public regarding computer crime	6
Better training for law enforcement in computer crime investigations	4
Increased prosecution of perpetrators when identified	3
More severe criminal penalties for computer crime perpetrators	5