A Study of the Proliferation of Computer Crimes

Lauren Smith
Kai S. Koong
Lai C. Liu
Computer Information Systems, Southern University at New Orleans
New Orleans, LA, 70126, USA
and
Robert Rottman
Kentucky State University
Frankfort, KY, 40601, USA

Abstract

The proliferation of computer crimes is a critical management issue for companies and organizations around the globe. This study examines the monetary losses of 13 categories of computer crimes for the period 1997 through 2000 as reported by the Computer Security Institute (CSI) and the Federal Bureau of Investigation (FBI). Specifically, this research examines the trend, magnitude, and direction for each of the different categories of computer crime. In addition, the total cost of computer crime over a four-year period was analyzed. The outcomes of this research should be most helpful to information systems administrators who are responsible for formulating information systems control strategies. Network and security administrators, Webmasters, and law enforcement officers of federal and state agencies such as the Federal of Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), and the Telecommunications Commission of the various states will find the analysis contained in this report insightful. Individuals involved with analyzing and securing corporate information resources such as computer consultants, systems analysts, systems developers, software engineers, and security experts will find the results meaningful. Educators and security scholars will find the outcomes reported in this study useful for the development of instructional material as well as the formulation of training strategies.

Keywords: Computer crimes, information systems security, computer security

Like the industrial revolution, the invention of the computer brought about major changes in the way government, corporations, and non-profit agencies operate. The addition of the Internet in the last quarter of the Twentieth Century has further revolutionized the view organizations have developed toward computer technology. Irrespective of an organization's area of specialization, computer technology is now a strategic asset for revenue generation, cost reduction, automation, and decision making. For these reasons, computer systems and the Internet have become a critical element in the social and economic infrastructure of organizations (Erwin 2000).

Unfortunately, as with every good technology, computer technology can be abused. Criminals have also found that this user-friendly technology can be a powerful instrument to commit illegal acts. Common types of crimes committed using computer technology include (O'Brien 1999; Power 2000a):

- Theft of money, services, software, hardware, and data.
- Destruction and alteration of files using viruses, worms, logic bombs and Trojan horses.
- Sabotage.
- Malicious access (example: hacking).
- Violations of privacy.
- Denial of services.
- Masquerading.

Each type of computer crime indicated above has resulted in increasingly costly damages annually. The types of perpetrators committing the crimes are also getting more diverse. For example, the famous Volkswagen AG case in 1987 involved theft of $253 million by company executives. An infamous case in

1994 involved a Russian hacker and his accomplices in St. Petersburg. Using the Internet, they broke into Citibank's mainframe system in New York and stole $11 million (Neumann 1995). According to the Computer Security Institute Report covering the period 1997 through 2000, monetary losses in reported cases of computer crimes have exceeded $600 million in the United States alone. Compared to the total number of computer crime cases, the majority of which were not reported or detected, this monetary loss can most probably be viewed as "the tip of the iceberg" (Power 2000b).

1. STATEMENT OF THE PROBLEM

Computer crimes have become key management issues since the early 1970s and they remain so in modern times (Loch et al. 1992; Bock & Schrage 1993; Weiss 1974). However, technological development and innovations in the business environment have resulted in changes in the nature of computer-related crimes (Wilson et al. 1992). Crimes committed during the beginning of the computer revolution were targeted at attaining monetary gains and tended to involve the theft of money.

Recent occurrences of crimes are committed by a more diverse group of criminals and their acts may be motivated by a variety of factors other than money. Insiders committed many of the early crimes. Outsiders who succeed in intruding into computer systems could often be traced to persons living near the facility and who have targeted a specific company to commit a crime. On the other hand, persons living in one country can easily commit a computer crime in another country. Furthermore, the target may be a specific company but the effect can be on the whole world.

Finally, but sadly, attitudes toward some forms of computer crimes need not be negative. Hackers, for example, consider their behavior to be "purely an intellectual activity" (Corbitt 2000; Freedman 1993). As a matter of fact, some hackers consider themselves to be industry watchdogs that are merely keeping a vigilant eye on unscrupulous vendors and tyrannical governments (Taylor 2000).

Irrespective of motive and cause and effect, the results and outcomes are the same. These crimes involved substantial monetary losses, man-hours wasted, and goodwill foregone (Neumann 2000; McCune 1998; Didio 1998). According to the Federal Bureau of Investigation (FBI), white-collar crime is the fastest-growing type of illegal activity in the United States (Martin 1998). Computer crime is a type of white-collar crime.

With the increasing number and types of new computer crimes occurring, managers and educators must have an understanding about the direction, magnitude, and different categories of computer crimes committed. Such an understanding can help them to become more focused when devising curriculum and prevention programs for training information systems security personnel in the workplace.

2. STATEMENT OF OBJECTIVE

As the number and complexity of computer applications proliferate, computer crimes will also continue to grow at an accelerated rate (Lee 1997). The growth will be in numbers as well as in level of sophistication. This research project examines the growth in the different types of computer crimes as reported by the Computer Security Institute (CSI) Annual Report for the period 1997 through 2000. Specifically, this study analyzes the trends, magnitude, and direction of the growth of the different categories of computer related crimes.

The outcomes of this research should be most helpful to information systems administrators in companies who are responsible for formulating information systems control strategies for their organizations. These administrators include the Chief Information Officer, the Chief Knowledge Officer, and the Chief Intelligence Officer. Network and security administrators, Webmasters, and law enforcement officers of federal and state agencies such as the Federal of Bureau of Investigation (FBI), the Central Intelligence Agency (CIA) and the Telecommunications Commission of the various states will find the analysis contained in this report insightful. Individuals involved with detecting and securing corporate information resources such as computer consultants, systems analysts, systems developers, software engineers, and security experts will find the results meaningful. Educators and security scholars will find the outcomes reported in this study useful for the development of instructional material as well as the formulation of training strategies.

3. DATA GATHERINGS

Every year, CSI conducts a survey of computer security crime occurrences and losses incurred by individuals who are classified as computer security practitioners. These persons are employed in a wide range of corporations and governmental agencies throughout the United States. The majority of the corporate participants work in financial institutions, high-tech firms, medical facilities, telecommunication providers, and utility companies. The participants employed in the public sector are distributed among local state, and federal government agencies.

The data for the period 1997 through 2000 are contained in the publication called *Computer Security Issues & Trends*. Both the Computer Security Institute (CSI) and the San Francisco Federal Bureau of Investigation (FBI) Computer Intrusion Squad collected this data set. All the thirteen categories of computer reported crimes contained on pages 8 and 9 of the Spring 2000 issue

were included in this study. The thirteen types of computer crimes are:

- Theft of proprietary information.
- Sabotage of data or networks.
- Telecommunication eavesdropping.
- System penetration by outsider.
- Insider abuse of Net access.
- Financial fraud.
- Denial of service.
- Spoofing (example: impersonate).
- Virus.
- Unauthorized insider access.
- Telecommunication fraud.
- Active wiretapping.
- Laptop theft.

It is important to point out that these figures include only quantifiable amounts reported by respondents. The annual survey was sent to 4,284 individuals, but 643 responses were received with a 15 percent response rate in 2000. In 1999, 3,670 surveys were sent, but 521 responses were received with a response rate of 14 percent. In 1998, 3,890 surveys were sent, but 520 responses were received with a 13 percent response rate. In 1997, 563 surveys were sent, but 563 responses were received with an 11 percent response rate. Some of the recipients may not have incurred any loss during a given year. Other recipients may have decided not to participate that year. Finally, some respondents may have not reported a monetary loss because they did not know how to quantify the losses. For example, 74 percent of the respondents acknowledged financial losses in 2000. However, only 42 percent of them could quantify the losses.

5. METHOD OF ANALYSIS

Each increment or decrement between years was computed by its difference and dividing the difference by the previous year and multiplying it by 100. The impact of crime types to the total cost was computed by dividing each type of crime cost by the total cost of crime for the respective years and multiplying it by 100. Finally, indexing was done to further demonstrate the impact, magnitude, and direction in the behavior of these computer crimes. The index was computed by dividing the observed year over the base year and multiplying the result by 100. All the trends exhibited by the different categories of computer crimes and the total crime costs during the period 1997 through 2000 were presented using tables that showed the magnitude of the annual changes.

6. FINDINGS

Three types of crimes showed similar trends all four years. All the three crime categories exhibited double digit proportions of the total. These three crime categories were insider abuse of Net access, virus, and laptop theft. Collectively, all three categories together accounted for over 50 percent of all the reported crime cases each year. Based on this observation, it can be said that the majority of the crimes are concentrated in three of the thirteen categories.

There were at least three other major observations identified in Table 1. First, there were no spoofing related crimes reported after 1997. It appeared that this crime was no longer a threat after that year. Second, there was a major increase in the number of crimes reported in 2000. Third, financial fraud accounted for about 5 percent of all the reported crime cases each year. Other details of quantified losses reported from the respondents during the four years were presented in Table 1.

Table 1. Number and Percent of Respondents with Quantified Losses

Category	1997		1998		1999		2000	
	No	%	No	%	No	%	No	%
Theft of proprietary information	21	4	20	4	23	4	22	3
Sabotage of data or networks	14	3	25	4	27	5	28	4
Telecom eavesdropping	8	1	10	2	10	2	15	2
System penetration by outsider	22	4	19	3	28	5	29	5
Insider abuse of Net access	55	10	67	12	81	15	91	14
Financial fraud	26	5	29	5	27	5	34	5
Denial of service	NA	0	36	6	28	5	46	7
Spoofing	4	1	NA	0	NA	0	NA	0
Virus	165	31	143	25	116	21	162	25
Unauthorized insider access	22	4	18	3	25	5	20	3
Telecommu-nication fraud	35	7	32	6	29	5	19	3
Active wiretapping	NA	0	5	1	1	0	1	0
Laptop theft	165	31	162	29	150	28	174	27
Total Number of Losses	537	100	566	100	545	100	641	100

Note: [NA] = Not Available, and [No] = Number Reported.

Table 2. Amount and Percentage of Each Type of Crime

Category	1997		1998		1999		2000		Total Crime Cost	%
	Amount	%	Amount	%	Amount	%	Amount	%		
Theft of proprietary information	20,048,000	20	33,545,000	25	42,496,000	34	66,708,000	25	162,797,000	26
Sabotage of data or networks	4,285,850	4	2,142,000	2	4,421,000	4	27,148,000	10	37,996,850	6
Telecom Eavesdropping	1,181,000	1	562,000	0	765,000	1	991,200	0	3,499,200	1
System penetration by outsider	2,911,700	3	1,637,000	1	2,885,000	2	7,104,000	3	14,537,700	2
Insider abuse of Net access	1,006,750	1	3,720,000	3	7,576,000	6	27,984,740	11	40,287,490	6
Financial fraud	24,892,000	25	11,239,000	8	39,706,000	32	55,996,000	21	131,833,000	21
Denial of Service	0	0	2,787,000	2	3,255,000	3	8,247,500	3	14,289,500	2
Spoofing	512,000	1	0	0	0	0	0	0	512,000	0
Virus	12,498,150	12	7,874,000	6	5,274,000	4	29,171,700	11	54,817,850	9
Unauthorized insider access	3,991,605	4	50,565,000	37	3,567,000	3	22,554,500	9	80,678,105	13
Telecom fraud	22,660,300	23	17,256,000	13	773,000	1	4,028,000	2	44,717,300	7
Active Wiretapping	0	0	245,000	0	20,000	0	5,000,000	2	5,265,000	1
Laptop theft	6,132,200	6	5,250,000	4	13,038,000	11	10,404,300	4	34,824,500	6
Total Losses	100,119,555	100	36,822,000	100	123,776,000	100	265,337,940	100	626,055,495	100

An analysis of the magnitude and mode of change in Table 2 showed some extremely frightening results. First, the amount of reported total loss more than doubled between 1999 and 2000. Second, in each given year, there are at least three types of crimes that reported double digit loss percentages. Third, during each of those years, these larger crime categories accounted for over 50 percent of all the total damages. Finally, over the four-year period, theft of proprietary information has the largest amount of losses. Crimes in the financial fraud and unauthorized insider access categories were the two other leading categories that exhibited the most financial losses. Particularly in the year 2000, there were a number of interesting observations. The number of crime groups showing double-digit loss percentages increased to five. The magnitude of change in several of the crime categories from the previous year was extremely dramatic. For example, active wiretapping losses came to only $20,000 in 1999. In 2000, it was $5 million. In 1999, unauthorized insider access losses were about $3.6 million. In 2000, it was over $22 million.

Indexing was used to further study the mode and speed of growth of each of the crime categories over the period studied. The monetary data from 1997 was selected as the base year. As seen from Table 3 below, two crime categories demonstrated the most aggressive growth patterns. Insider abuse of Net access grew from a base index of 100 in 1997 to an index of 2,780 in 2000. Active wiretapping grew from a base index of 100 in 1998 to an index of 2,041 in 2000. Two categories of crimes showed a receding trend. Telecom eavesdropping receded from a base index of 100 in 1997 to an index of only 84 in 2000. Telecom fraud showed the biggest decrease. In 2000, the index was 18.

Analysis of individual crime categories also revealed several other very interesting trends. First, theft of proprietary information grew continuously from the base year. Insider abuse of Net access and active wiretapping are the two categories that showed the largest index growth. Some of these categories appear to fluctuate widely. For example, sabotage of data or networks and financial fraud fell to an index of 50 and 45 respectively in 1998, but has exhibited continuous growth since then. Unauthorized insider access had the highest index with 1,267 in 1998, but fell in 1999, and then increased again in 2000. Finally, spoofing showed zeros because there was no data reported after 1997.

Table 3. Trend Analysis of Each Crime Using 1997 as the Base Year

Category	1997 Index	1998 Index	1999 Index	2000 Index
Theft of proprietary information	100	167	212	333
Sabotage of data or networks	100	50	103	633
Telecom eavesdropping	100	48	65	84
System penetration by outsider	100	56	99	244
Insider abuse of Net access	100	370	753	2780
Financial fraud	100	45	160	225
Denial of service	0	100	117	296
Spoofing	100	0	0	0
Virus	100	63	42	233
Unauthorized insider access	100	1267	89	565
Telecom fraud	100	76	3	18
Active wiretapping	0	100	8	2041
Laptop theft	100	86	213	170

Table 4. Trend Analysis of Each Crime Using Percentages

Category	1997-1998 Percent	1998-1999 Percent	1999-2000 Percent
Theft of proprietary information	67	27	57
Sabotage of data or networks	-50	106	514
Telecom eavesdropping	-52	36	30
System penetration by outsider	-44	76	146
Insider abuse of Net access	270	104	269
Financial fraud	-55	253	41
Denial of service	0	17	153
Spoofing	0	0	0
Virus	-37	-33	453
Unauthorized insider access	1167	-93	532
Telecom fraud	-24	-96	421
Active wiretapping	0	-92	24900
Laptop theft	-14	148	-20
Total Costs	37	-10	114

Table 4 showed the percent of growth between the respective years was analyzed to further examine the magnitude and mode of the data pattern. There were a few interesting observations:

1. Insider abuse of Net access showed a consistent growth pattern throughout the period in the form of triple digit percentages.
2. The number of categories reporting at least a double-digit percentage growth pattern increased from three to six from 1997 through 2000.
3. Between 1999 and 2000, the change in total loss exceeded 100 percent for the first time.
4. The ranges were extremely dramatic in 1999. Between 1997 and 1998, the ranges were between –55 percent and 1167 percent. Between 1999 and 2000, the ranges were between –20 and 24,900.

7. SUMMARY

This study found that the different types of computer crime exhibited a variety of behavioral trends. Some were increasing continuously. Others increased or decreased in the last year observed. Total losses each year were dominated by three types of crimes: theft of propriety information, financial fraud, and unauthorized insider access. Magnitude as well as direction of change can be extremely dramatic. Some of the major observations are presented below:

- Three categories of computer crime were responsible for over 50 percent of the total costs. The three categories were theft of propriety information, financial fraud, and unauthorized insider access.
- Three categories of computer crime were increasing continuously each year. These crimes were theft of proprietary information, insider abuse of Net access, and denial of service.
- In the most recent year examined, the magnitude of change in the different types of crimes examined can be extremely dramatic. When indexing was used, the changes can be as great as about 28 times the base year. Active wiretapping and Insider abuse of Net access showed a substantially large index of 2,041 and 2,780 in 2000.
- Some of the losses incurred between two immediate years can also be fairly dramatic. Active wiretapping showed a 24,900 percent increase between 1999 and 2000. Unauthorized insider access showed a 1,167 percent increase between 1997 and 1998.
- Compared to the previous two periods examined, total losses incurred between 1999 and 2000 were substantially larger. Total losses increased 114 percent. Losses in the previous two periods, 1997-1998 and 1998-1999, were 37 percent and -10 percent respectively. Eight of the 13 types of crimes showed more than a 100 percent increase in losses between 1999 and 2000.

8. CONCLUSIONS

This study found the losses were concentrated in certain categories and there were certain identifiable trends. However, the trends exhibited using the absolute monetary losses examined here were not sufficient to tell the whole story. For example, laptop theft had the most quantifiable losses reported. This category of crime was not the top three types of crimes when monetary figures were examined. The percentages and indexes analyzed in this research also provided a wealth of other information that was especially meaningful. It is therefore wise to use a variety of analytical techniques to examine the data because such techniques can provide the reader with a more holistic view of the problem examined.

The data from the year 2000 should especially alarm and raise warning to managers as well as educators. Some of the quantified crimes as well as the amount of monetary damages reported were extremely dramatic. If the year 2000 is an indication of problems down the road, managers must begin to devise contingency plans immediately to minimize this problem. To better prepare students about computer crimes that are showing this increase in number and magnitude, educators may want to increase their coverage of information systems security topics in their curricula.

9. CAVEATS

The data covered only the period 1997 through 2000. Given the short period studied, it was not possible for any cyclical trends to be identified. Only those crimes that showed continuous growth or decline patterns and those that exhibited dramatic changes were identified and reported.

Like all studies that are dependent on survey data, there are several limitations to the findings in this research. First, the trends identified are based on quantifiable cases reported to the CSI and FBI. The response rate and the participants to each of the four years are different. Companies that have incurred a loss but elected not to participate in the study during the respective years are not captured in the findings. Second, companies that incurred a loss but were not included in the targeted database were also not included. The proportion of companies in both these cases and the total actual number of cases are unknown. If the proportions of unreported cases are significant, it could have affected the trends identified. Despite these limitations, the findings reported were significant and without compromise. The data set used was a reputable one and the method used for analyzing the data was robust. Moreover, great caution was also taken in interpreting the results.

10. REFERENCES

Bock, D.B. and J. F. Schrage, 1993, "Computer Viruses: over 300 Threats to Micro-Computing … And Still Growing." Journal of Systems Management, 19, pp. 8-13.

Corbitt, T., 2000, "Stop the Hacker." Journal of the Institute of Credit Management, April, pp. 22-23.

DiDio, Laura, 1998, "Ex-employee Nabbed in $10M Hack Attack." Computerworld, 32, p. 6.

Erwin, Dan, 2000, "Data Security Seen Crucial for E-Commerce Success." National Underwriter, 104, pp. 9-12.

Freedman, David H., 1993, "The Goods on Hackers Hoods." Forbes, September, p. 32.

Lee, Wanbil W., 1997, "A Deterrent Measure Against Computer Crime: Knowledge-Based Risk-Analytic Audit." Singapore Management Review, 19, pp. 19-45.

Loch, K. D., H. H. Carr, and M. E. Workentin, M., 1992, "Threats to Information Systems: Today's Reality, Yesterday's Understanding." MIS Quarterly, June, pp. 137-186.

Martin, Josh, 1998, "Dissecting the Books." Management Review, 87, p. 47.

McCune, Jenny C. (1998). How Safe is your Data? Management Review, 87, 17-21.

Neumann, Peter G., 1995, Computer-Related Risks. (pp. 132-180). ACM Press, New York

Neumann, Peter G., 2000, "Denial-of-service Attacks." Communications of the ACM, 43, p. 136.

O'Brien, James, 1999, Managing IT Security and Ethical Challenges. Irwin McGraw-Hill, New York.

Power, Richard, 1999, "1999 CSI/FBI Computer Crime and Security Survey." Computer Security Issues & Trends, 5, pp. 1-15.

Power, Richard, 2000a, Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace. QUE Publishing, Indiana.

Power, Richard, 2000b, "Viruses, Attacks, and Sabotage: It's a Computer Crime Wave Crime of Many Kinds is Dropping These Days--Except When it Comes to Computers and Cyberspace." Fortune Magazine, 141, p. 484.

Taylor, Chris, 2000, "Behind the Hack Attack." Time, 155, pp. 44-47.

Weiss, H., 1974, "Computer Security: An Overview." Datamation, April, pp. 42-47.

Wilson, J. L., Efraim Turban, and M. Zviran, 1992, "Information Systems Security: A Managerial Perspective." International Journal of Information Management, 12, p. 105.