Forecasting Computer Crime Complaints

Adnan Omar
aomar@suno.edu

Ada Kwanbunbumpen
adakwanbunbumpen@yahoo.com

David Alijani
dalijani@suno.edu
Computer Information Systems Department
Southern University at New Orleans
New Orleans, Louisiana, 70126, USA

Abstract

Computer crime forecasts unethical behavior in the business environment, as well as, in society as a whole. Today's society is extant with countless examples of how destructive and far-reaching unethical actions can be. From large-scale embezzlement and fraud in the business world to unethical computer conduct, unethical behavior destroys society's moral fiber. The principle function of this paper is to gather and investigate related unethical computer activities, examine the trend of unethical behavior from data collected to forecast computer crime complaints, and recommend ways to minimize the ever-growing phenomenon of computer crime. The goal of this research is to forecast the incidence of computer crime based on given data using the linear regression equation. The results of this study indicate the potential of increasing computer crimes. Minimizing computer crime requires a combination of aggressive legislation, new technology solutions, and increased public awareness.

Keywords: computer crime, ethics, linear regression, security, technology

1. INTRODUCTION

The birth of computers to society has created possibilities for individual and institutional behavior that did not exist before. However, computers, like other technology advances produce both potential advantages and disadvantages to society. The computer creates a much greater capacity to keep a watch on individuals without their knowledge. Furthermore, the computer has also developed a more grotesque weapon system; consequently, eliminating the need for human contact in many activities. There is no question that the use of information technology in business presents major security challenges, poses serious ethical questions, and affects society in significant ways (O'Brien, 2001).

Computer crime creates a severe risk to America's national security. Recently, highly publicized computer virus attacks have exposed computer crime as an increasing dilemma. Sensational headlines, such as "Nation Faces Grave Danger of Electronic Pearl Harbor," "Internet Paralyzed by Hackers," and "Computer Crime Costs Billions" have become common. Law enforcement organizations cannot determine exactly how many computer crimes occur each year (Goodman, 2001).

2. LITERATURE REVIEW

Abuse of the Internet continues to grow at an alarming rate. The Federal Bureau of Investigation (FBI) Chief stated at a Senate hearing that the number of computer crimes

doubled in 1997. In 1998, 547 cases on computer intrusion were opened. Later, the number of similar cases increased to 1154 in 1999. The FBI stated that the main threat came from the "computer experts, hackers, and virus founders who are not satisfied with their life or the way they live, so they hunt for money" (Freeh, 2000).

According to the United States of America's official statistics, it was found that of the 90% interviewed whose computer systems had undergone Internet attacks in 1999, 74% stated that penetration into their system was connected with embezzlement of confidential information or financial fraud. Financial losses from information embezzlement and financial fraud result in $68 million and $56 million, respectively. Financial losses of the 273 interviewed resulted in more than 265 million dollars. In 1998, the loss from attacks such as "service refusal" was $77,000 and dramatically increased up to $116,000 in 1999 (Freeh, 2000).

The advanced speed of technology has made it easier for computer criminals to conceal information about their crimes. Due to the complexity of the digital environment, evidence is collected and handled differently than it was in the past and often requires careful computer forensic investigation.

Crimes committed by computer users may cause damage or alteration to the computer system. Compromised computers may possibly be used to launch attacks on other computers or networks. The FBI makes use of many federal statutes to investigate computer crimes. The "FBI is sensitive to the victim's concerns about public exposure, so any decision to investigate is jointly made between the FBI and the United States Attorney in order to take the victim's needs into account" (How the FBI Investigates, 2004).

Preventive or deterrent measures are difficult in the cyber world, partly because of the ability of attackers to remain anonymous" (Shimeall et al, 2001, 2002). An unrestricted cyber-war offensive, however, would almost certainly give a few clues as to their identity. Computer network designs should integrate notions of robustness and survivability, while contingency plans for the continued implementation of critical roles and missions with far less cyber connectivity are important.

"Insulated intranets that can operate efficiently and safely without wider connections offer considerable promise in this respect" (Shimeall et al, 2001, 2002). The obstacles to enhanced network survivability are many and varied. Security is often an afterthought rather than an integral part of network design.

The government and businesses have different approaches to security and its provision. The lines of responsibility in the government have often been uncertain and confused by overlapped and competed jurisdictions. However, all complications can be overcome with a mixture of political will, organizational commitment, careful planning, and systematic implementation. "Defense planning needs to incorporate the virtual world, if there is to be any chance of limiting physical damage in the real world" (Shimeall et al, 2001, 2002).

The reason for the crime problem is that people have lost their moral conscience (Colson, 1991). Combating new computer security threats by stricter enforcement may be a superior solution to curtail computer crime. Such punishment will scare these perpetrators to think twice before attempting to conduct a computer crime. Another way to end such lawbreaking is to fine the computer savvy convict and donate the money to computer crime-stopper organizations and enforcers.

A "user must be aware that a determined and creative criminal can defeat nearly any security measure" (Standler, 1999). It is also possible to construe computer ethics as a wider topic to include the standards of professional practice, codes of conduct, aspects of computer law, public policy, and corporate ethics--even certain topics in the sociology and psychology of computing (Bynum, 2001).

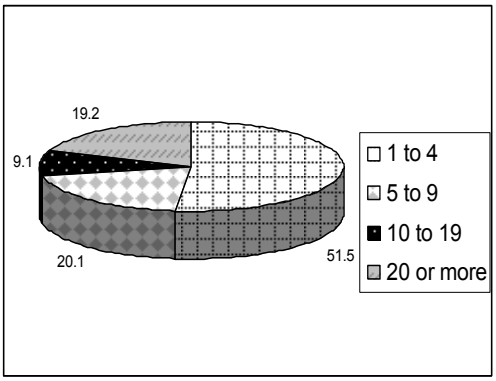
Numerous "crimes involving computers are no different from crimes without computers: the computer is only a tool that a criminal uses to commit a crime" (Standler, 1999, 2002). In 1986, the first computer virus, "in the wild" was found in a computer store in Lahore, Pakistan. In the 1980s, computer viruses were commonly spread through floppy disks from one user to another user. In the late 1990s, computer viruses were generally spread via the Internet, either by

e-mail or by downloaded programs from websites.

According to CNET News.com, "the FBI calculated the price tag by extrapolating results from a survey of 2,066 organizations … and found that 1,324 respondents, or 64 %, suffered a financial loss from computer security incidents over a twelve month period. The average cost per company was more than $24,000, with the total cost reaching $32 million for those surveyed" (Evers, 2006).

Figure 1 shows that almost a fifth of U.S. businesses said they suffered twenty or more incidents, such as virus infections, in an FBI survey of computer security incidents as companies in the past year (Evers, 2006).

Figure 1: U.S. Businesses Under Attack



Source: The 2005 FBI Computer Crime Survey

David Yale states that "the news has been happy to showcase various types of computer crime. From teen-age hackers to Internet prowling pedophiles, it seems that every week a new story breaks. As our world becomes more computerized and ever more interconnected, different kinds of computer crimes will continue to grow. Types of computer crimes include break-ins of computers to get trade secrets or other information that can be turned into profit, illegal entry for the thrill and challenge, confidence schemes, and the use of computers to meet and select victims of old-fashioned crimes. Additionally, more and more information that law enforcement officials will consider evidence will be stored on computers, and could add a new wrinkle to criminal investigations and trials" (Yale, 1997).

Table 1 shows that in the types of electronic crimes committed among the organizations experiencing attacks in 2003, virus or other malicious codes were the most frequent type (77%) followed by denial of service attacks (44%), i.e., imitating legitimate companies online in an effort to access confidential information.

Table 1: Types of Electronic Crimes

Virus or other malicious codes	77%
Denial of Service Attack	44%
Illegal generation of SPAM email	38%
Unauthorized access by an insider	36%
Phishing	31%
Unauthorized access by an outsider	27%
Fraud	22%
Theft of intellectual property	20%
Theft of other proprietary info	16%
Employee identity theft	12%
Sabotage by an insider	11%
Sabotage by an outsider	11%
Extortion by an insider	3%
Extortion by an outsider	3%
Other	11%
Don't know	8%

Source: 2004 E-Crime Watch Survey™ Findings

Bob Bragdon, Publisher of the Chief Security Officer (CSO) magazine, stated that "the increase in e-crime over the past year again demonstrates the need for corporate, government, and non-governmental organizations to develop coordinated efforts between their IT and security departments to maximize defense and minimize e-crime impact. There is a lot of security spending going on, but not much planning. It's essential for chief security officers and information technology pros to find the most manageable, responsive, and cost-effective way to stop e-crime from occurring" (E-Crime Watch, 2004).

Common types of computer crime are "fraud by computer manipulation, computer forgery, damage to or modification of computer

data or programs, unauthorized access to computer systems or services, and unauthorized reproduction of computer programs" (Maher, 2006). Most of these crimes are not new. Criminals simply devise different ways to undertake standard criminal activities such as fraud, theft, blackmail, forgery, and embezzlement using the new medium, often involving the Internet (Wikipedia, 2004, 2006).

3. OBJECTIVE

The objective of this project is to gather and investigate related unethical computer activities, examine the trend of unethical behavior from data collected to forecast computer crime, and recommend ways to minimize the ever-growing phenomenon of computer crime. The given data applied in the linear regression equation predicts the unethical behavior of computer crime.

4. HYPOTHESES

Given the data complaints from the Internet Crime Complaint Center (IC3) 2000, 2001, 2002, 2003, 2004, and 2005 National Crime Reports, the following null and alternative hypothesis were made:

H_0: The percentage of computer crime complaints for 2006 through 2008 will not increase.

H_a: The percentage of computer crime complaints for 2006 through 2008 will increase.

5. METHODOLOGY

To predict the number of complaints for the targeted years, the authors used Microsoft Excel to apply the linear regression equation mathematically. The process of prediction involves two steps. The first step was to determine the regression line, which is a mathematical equation. The second step was to use the mathematical equation to predict scores or complaints. Due to the limitation of discussion of linear regression, the mathematical equation is the equation of a straight line.

The mathematical equation of a straight line expresses a functional relationship between two variables. In predicting *Y* scores from *X* scores, the value of *Y* is a function of *X* and uses the slope-intercept form of the equation for a straight line.

The equation for a straight line used in prediction is $\hat{Y} = a + bX$

where

$\hat{Y}$ = predicted score
a = Y intercept
b = slope of the line
X = given score

The slope of a line is defined as the amount of change in *Y* that corresponds to a change of 1 unit in *X*. The slope of a line can be positive or negative and can be less than or greater than 1. The intercept of the line was defined as the value of *Y* where *X* equals 0 (Jurs, 1998). A Linear Regression (LR) line is a trend line that is drawn mathematically so that it represents the 'best fit' for the data points it passes through. The formulas use the least squares method to determine the line's placement to minimize the distances between the data points and the trend line (Arrington, 2006).

The first step was to calculate the value of *b* by using:

$$b = \frac{n\Sigma XY - \Sigma X \Sigma Y}{n\Sigma X^2 - (\Sigma X)^2}$$

After b was calculated, the next step was to calculate *a* by using:

$$a = \frac{\Sigma Y - b\Sigma X}{n} = \bar{Y} - b\bar{X}$$

where

n = total number of observations.

After both *a* and *b* were calculated, they were then substituted into the $\hat{Y}$ formula to predict the score or complaints for years 2006, 2007, and 2008. The results will be discussed in the findings section.

6. DATA COLLECTION

The IC3 is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C). It

serves as a means to receive Internet related criminal complaints, to further research, and to refer the criminal complaints to federal, state, local, or international law enforcement and/or regulatory agencies for any investigation they deem to be appropriate.

Data used in this research to predict the computer crime complaints per year were from the IC3 Annual Report of Internet Crime, originally known as the Internet Fraud Complaint Center (IFCC). Data used to predict the number of complaints for 2006, 2007, and 2008 were based on information that were provided to IC3 through the complaint forms submitted online at www.ic3.gov or www.ifccfbi.gov. Complaints were collected from January 1 through December 31 of each year since 2001. There were 16,838 filings in 2000. Although, the Internet Fraud Complaint Center (IFCC) did not begin taking complaints until May 8 of that year, the number of complaints filed per month averaged 6,255.

Given the availability of data, the use of information contained from the IC3 annual complaint statistics filed from 2000 through 2005, shown in Table 2, predicted targeted years.

Table 2: Yearly Computer Crime Complaints Received Via IC3 Website

Year	Complaints
2000	16,838
2001	49,711
2002	75,063
2003	124,509
2004	207,449
2005	231,493

The totals per year include many different fraudulent and non-fraudulent complaints, such as auction fraud, credit/debit card fraud, computer intrusions, unsolicited email (SPAM), and child pornography.

7. METHOD OF ANALYSIS

The data collected for the six consecutive years were analyzed accordingly by means of the quantitative technique using the linear regression equation. Microsoft Excel also allows the user to predict the average value for y for a specified value of x in a number of approaches. In this approach the user entered the regression formula in a worksheet cell and inserted the value or cell location of the value for the independent variable, x, into the formula. The cell would then display the predicted y value.

Formulas were used to compute and predict computer crime complaints for the following years: 2006, 2007, and 2008. Based on the data from 2000-2005, the predicted number of computer crime complaints for 2006 were calculated. After the 2006 forecast was calculated, the process was repeated to predict the number of computer crime complaints in 2007-2008 by incorporating it into the data table shown in Table 3.

Table 3: Forecasting 2008 Excel Formula Spreadsheet

	A	B	C	D	E
105	Forecasting 2008				
106					
107	Year	Time	Complaints		
108		Xi	Yi	Xi²	XiYi
109	2000	1	16838	=B109^2	=B109*C109
110	2001	2	49857	=B110^2	=B110*C110
111	2002	3	75063	=B111^2	=B111*C111
112	2003	4	124509	=B112^2	=B112*C112
113	2004	5	207449	=B113^2	=B113*C113
114	2005	6	231493	=B114^2	=B114*C114
115	2006	7	=277071.2	=B115^2	=B115*C115
116	2007	8	=B84	=B116^2	=B116*C116
117		Σ =SUM(B109:B116)	=SUM(C109:C116)	=SUM(D109:D116)	=SUM(E109:E116)
118		Xi	Yi	Xi²	XiYi
119					
120	xbar =	=B117/B123			
121	ybar =	=C117/B123			
122	∑ xi *yi=	=E117			
123	n=	8			
124	b=	=(E117-(B117*C117/B123))/(D117-(B117*B117/B123))			
125	a=	=B121-(B124*B120)			
126	Ŷi =	=B125+(B124*9)			
127	n*xbar^2=	=B123*(B120*B120)			
129					
132	Year	Complaints			
133	2000	16838			
134	2001	49857			
135	2002	75063			
136	2003	124509			
137	2004	207449			
138	2005	231493			
139	2006	=B31			
140	2007	=B84			
141	2008	=B126			

The percentage change between each year was calculated to test the null hypothesis as shown in Table 4.

Table 4: Percentage Change in Excel Spreadsheet for 2000 through 2005

	A	B	C
129	**Year**	**Complaints**	**% Change**
130	**2000**	*16,838.00*	
131	**2001**	*49,957.00*	297%
132	**2002**	*75,063.00*	150%
133	**2003**	*124,509.00*	166%
134	**2004**	*207,449.00*	167%
135	**2005**	*231,493.00*	112%

Once a good fitting relationship was found, it was used to predict the average value for y for a specified value of x. Another approach in Excel was the statistical function called TREND. The general format for this function is:

=TREND (range of y values, range of x values, range of x values to be used for predicting).

The trend is the long-run shift or movement in the time series observable over several periods of time (Anderson et al, 1996). The TREND function allowed the user to select the range of values from Table 5.

Table 5: Forecast Computer Crime Complaints in Formula View Using the TREND Function

	A	B
1	TREND Function	
2		
3	pg 93-94	
4		
5	Year	Given Complaints
6	2000	*16838*
7	2001	*49957*
8	2002	*75063*
9	2003	*124509*
10	2004	*207449*
11	2005	*231493*
12		
13		
14		
15	Year	Forecasted Complaints
16	2006	=TREND(B6:B11,A6:A11,A16:A18)
17	2007	=TREND(B6:B11,A6:A11,A16:A18)
18	2008	=TREND(B6:B11,A6:A11,A16:A18)

The second and subsequent predicted *y* values were subsequently computed as shown in Table 6.

Table 6: Forecast Computer Crime Complaints in Output View Using the TREND Function

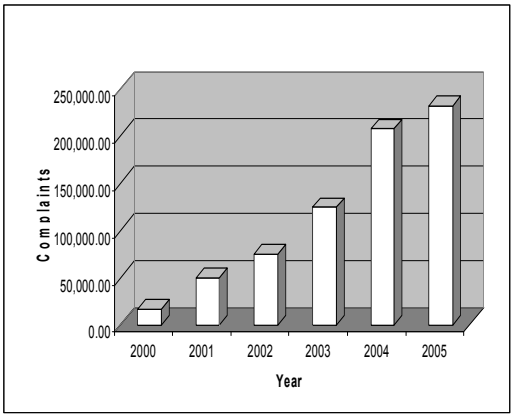
	A	B
16	2006	277,071.20
17	2007	322,648.26
18	2008	368,225.31

The TRENDLINE method was also used to obtain the regression analysis as demonstrated. Another way to find the predicted values was through the REGRESSION analysis tool.

8. FINDINGS

After acquiring the given data for five consecutive years from IC3's Annual Reports, shown in Figure 2, the linear regression formula was applied to forecast the computer crime complaints for the years 2006, 2007, and 2008.

Figure 2: Yearly Comparison of Computer Crime Complaints Received Via IC3



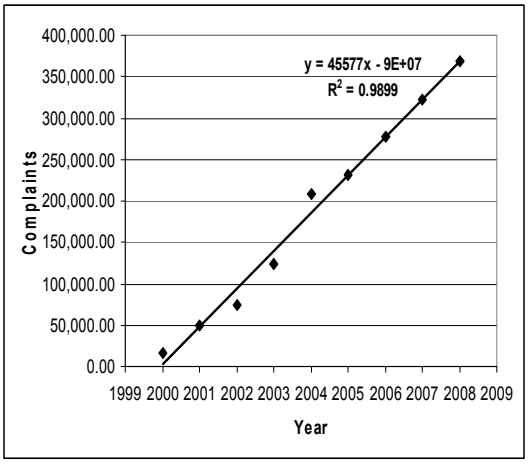
Source: IC3 National Crime Report

9. ANALYSIS OF OUTCOMES

Given the data complaints from the IC3's 2001 through 2005 Annual National Crime Report, the Microsoft Excel Workbook was made to test null and alternative hypothe-

ses. Figure 3 was created to show the trend line in the first approach in predicting the computer crime complaint values using the data.

Figure 3: Forecast Complaints Trend Line

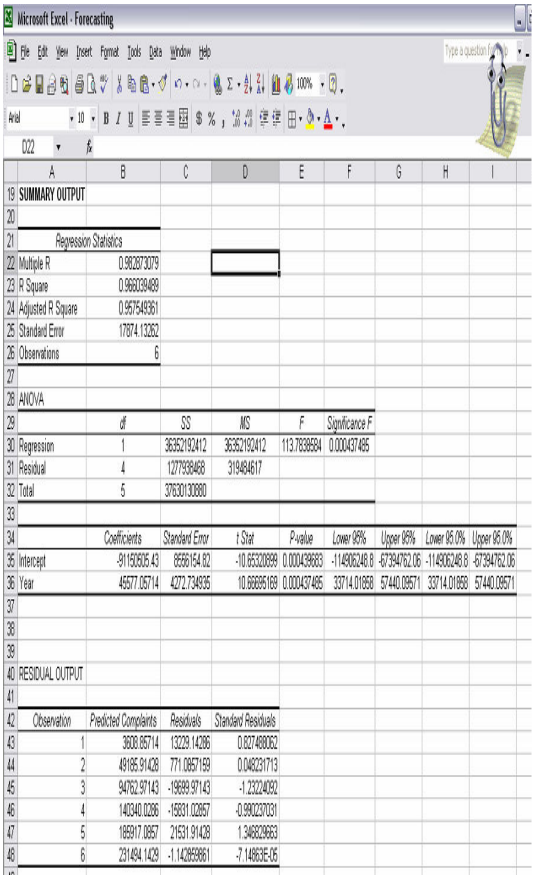


First of all, in Figure 3, the increasing trend line showed the best relationship for this data as the equation *y = 45577x - 9E + 07,* where *x,* is the year in number of computer crime complaints and y is the number of computer crime complaints. Secondly, the coefficient of determination, R^2*= 0.9899*, suggested that 98% of the variability of computer crime complaint values about the average can be explained by changes in computer crime complaints, which indicates that the equation fits the data very well. Therefore, R^2 is a good single measure of the strength of the relationship. In summary, the simple linear regression analysis yielded a scatter diagram providing a visual interpretation of the relationship between two variables: the equation for the straight line relationship, and R^2, a good measure of strength of the linear relationship.

In the second approach for prediction, the statistical function called, TREND, was used to generate forecast values. The values generated by Excel's TREND function yielded the same results for the first approach. The statistical function is an alternative method to predict complaint values for as many years as needed.

In the third approach for predicting computer crime complaints, using the Regression Analysis Tool, output is generated by Excel as shown in Table 7.

Table 7: Results for Forecast Computer Crime Complaints Using the Regression Analysis Tool



Microsoft Excel - Forecasting

	A	B	C	D	E	F
19	SUMMARY OUTPUT					
20						
21	*Regression Statistics*					
22	Multiple R	0.98287079				
23	R Square	0.96603489				
24	Adjusted R Square	0.95754361				
25	Standard Error	17874.13262				
26	Observations	6				
27						
28	ANOVA					
29		*df*	*SS*	*MS*	*F*	*Significance F*
30	Regression	1	3635219241.2	3635219241.2	113.7639584	0.000437465
31	Residual	4	127739848.8	31934961.7		
32	Total	5	3763013088			
33						
34		*Coefficients*	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*
35	Intercept	-91155605.43	9556154.82	-10.65320899	0.000439683	-114906248.8
36	Year	45577.05714	4272.734935	10.66895169	0.000437465	33714.01658
37						
38						
39						
40	RESIDUAL OUTPUT					
41						
42	*Observation*	*Predicted Complaints*	*Residuals*	*Standard Residuals*		
43	1	3808.857143	13229.14286	0.827498062		
44	2	49185.91429	771.0857159	0.048231713		
45	3	94762.97143	-19999.97143	-1.252024182		
46	4	140340.0286	-19931.02857	-0.990237031		
47	5	185917.0857	21531.91429	1.346829663		
48	6	231494.1429	-1.142857661	-7.14863E-05		

	G	H	I
34	*Upper 95%*	*Lower 95.0%*	*Upper 95.0%*
35	-67394762.06	-114906248.8	-67394762.06
36	57440.09571	33714.01658	57440.09571

The numerical output of Table 7 is presented in four parts from top to bottom. The top result, labeled Regression Statistics, presented the values for the coefficient of correlation *r*, labeled as Multiple R. The coefficient of determination, r^2, is labeled as R Square; the *adjusted* r^2 labeled as Adjusted R Square the standard error of the estimate is labeled as Standard Error; and the sample size is labeled as Observations. The second result, found under the label ANOVA, provided an analysis of variance output for the regression. The third result presented the regression coefficients together with statistics for evaluating the significance of the coefficients, such as the t statistic values, p-values, and confidence intervals. Finally, the bottom result, labeled Residual Output, pro-

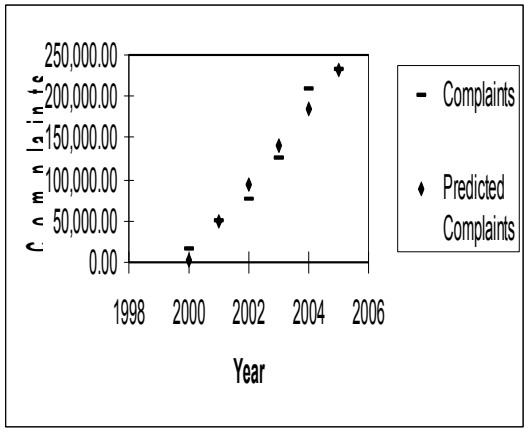
vided the predicted *y* values for each of the data points in the sample along with the residual and standardized residuals.

Statistical values were given for testing the significance of the relationship with the p-value approach. From the ANOVA table's output, the value for the F statistic was 113.78 in cell E30, with a corresponding Significance F value of 0.000437485 in cell F30. The Significance F was the p-value for the overall regression relationship categorized as "Very Highly Significant." Thus, rejecting the null hypothesis, concluding that it is a good relationship based on the given data.

In a simple linear regression analysis, the same conclusions can be reached based on the t statistic for the regression coefficient for computer crime complaints. The year coefficient was 45577.05714 in cell B36 with a t statistic value of 10.66695169 in cell D36 and a corresponding p-value 0.000437485 in cell E36.

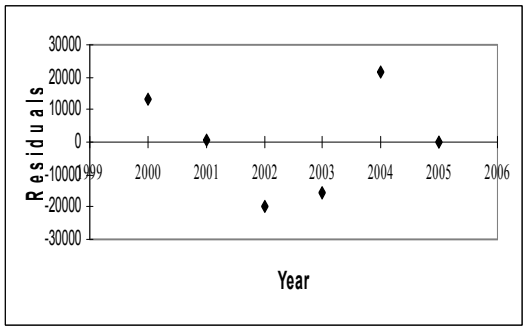
For simple linear regression, the p-values for this t statistic and for the prior F statistic will always be exactly the same. The relationship was statistically significant. The line fit plot of Figure 4 was similar to the scatter diagram of Figure 5. However, Figure 4, shown below did not show a line of predicted y values. Instead, it showed the predicted y value for each of the x values of the input data.

Figure 4: Year Line Fit Plot



The residual plot in Figure 5 is useful for identifying outliers and for determining whether the assumptions underlying the regression analysis were met or not.

Figure 5: Year Residual Plot



As in the simple linear regression with the regression analysis tool, the predicted average values for y were found by inserting the regression formula in a worksheet cell or by using the TREND function.

10. CONCLUSIONS

According to the data from the IC3 annual reports, the number of computer crime complaints increased from the year 2000 to 2005. Using Microsoft Excel, the authors applied the following procedures to predict the complaints for the forecasted years:

1) The linear regression formula
2) The statistical function called TREND
3) The simple linear regression method using the Regression Analysis Tool

In the first method, the mathematical formula, $\hat{Y} = a + bX$, was used to predict the values for the years 2006 through 2008. The second method yielded the same results but with a scatter plot designed to show the increasing trend line. The output for the third method was also the same as both the first and second methods. However, the simple linear regression method using the Regression Analysis Tool also created a more detailed report for statistical significance testing which included the ANOVA table, Significance F, and p-value.

In the third approach, the ANOVA table showed that the Significance F was the p-

value, 0.000437485, for the overall regression relationship. This p-value was categorized as "Very Highly Significant". Thus, the authors are able to reject the null hypothesis and accept the alternative hypothesis, concluding, that there is a good relationship based on the given data. This indicates that there is a positive relationship between advancing years and the incidence of computer crime.

H_0: The percentage of computer crime complaints for 2006 through 2008 will not increase. (reject)

H_a: The percentage of computer crime complaints for 2006 through 2008 will increase. (accept)

Abuse of the Internet continues to grow at an alarming rate. The findings of this study testify to the need for computer ethics to be taught at all educational levels as well as in the workforce. Teaching computer ethics at all levels will allow students and workers to act and think ethically.

Obviously, in many ways, technology offers tremendous opportunities for the malicious computer users to engage in unethical computer activities. Indeed, computer crime is a global problem. International computer laws may be combined with current United States computer laws to ensure a much greater enforcement worldwide. Moreover, strictly enforcing these laws for computer crime perpetrators is strongly suggested as a way to prevent those computer users from committing computer crimes.

11. REFERENCES

Anderson, D. R., Sweeney, D. J., and Williams, T. A. (1996). Chapter 18: Forecasting. Business Statistics for Business and Economics. West Publishing Company: New York.

Arrington, H. (2006). Trading Tip: Linear Regression Explained. Retrieved April 13, 2006, from the World Wide Web: http://www.ensignsoftware.com/tips/tradingtips54.htm

Bynum, T. (2001). Computer Ethics: Basic Concepts and Historical Overview. The Stanford Encyclopedia of Philosophy (Winter 2001 Edition).

Colson, C. W. (1991). Right or Wrong in Today's Society: The Problem of Ethics. Harvard Business School, Boston, Massachusetts.

2004 E-crime Watch™ Survey Shows Significant Increase in Electronic Crimes: 2003 E-Crime Losses Estimated At $666 Million. Retrieved March 31, 2006, from the World Wide Web: http://www.csoonline.com/releases/ecrimewatch04.pdf

Evers, J. (2006). Computer crime costs $67 billion, FBI says. CNET News.com. Retrieved March 31, 2006, from the World Wide Web: http://news.com.com

Freeh, L. J. (2000). Statement for the Record of Director Federal Bureau of Investigation on Ñybercrime Before the Senate Committee on Judiciary Subcommittee for the Technology, Terrorism, and Government Information Washington, D.C. Retrieved March 30, 2006, from the World Wide Web: http://www.fbi.gov/pressrm/congress/congress00/vatis022900.htm

Goodman, M. (2001). Making Computer Crime Count. FBI Law Enforcement Bulletin. 70. 8.

How the FBI Investigates Computer Crime. (2004). Carnegie Mellon University Retrieved March 27, 2006, from the World Wide Web: http://www.cert.org/tech_tips/FBI_investigates_crime.html#ccinv

Jurs, H. W. (1998). Chapter 6: Linear Regression Prediction. Applied Statistics for the Behavioral Sciences. New York: Houghton Mifflin Company.

Maher, L. (2006). Proving Your Case - Computer Security. Retrieved March 22, 2006, from http://www.certconf.org/presentations/1999/brief/brief.htm

National White Collar Crime Center. (2004). IC3 2003 Internet Fraud Report. Retrieved April 11, 2006, from the World Wide Web: http://www.ic3.gov/media/annualreports.aspx.

National White Collar Crime Center. (2005). IC3 2004 Internet Fraud Report. Retrieved April 11, 2006, from the World Wide Web: http://www.ic3.gov/media/annualreports.aspx.

National White Collar Crime Center. (2006). IC3 2005 Internet Fraud Report. Retrieved April 11, 2006, from the World Wide Web: http://www.ic3.gov/media/annualreports.aspx.

National White Collar Crime Center. (2002). IFCC 2001 Internet Fraud Report. Retrieved April 11, 2006, from the World Wide Web: http://www.ic3.gov/media/annualreports.aspx.

National White Collar Crime Center. (2003). IFCC 2002 Internet Fraud Report. Retrieved April 11, 2006, from the World Wide Web: http://www.ic3.gov/media/annualreports.aspx.

O'Brien, J. A. (2001). Management Information Systems. 5th ed. 380.

Shimeall, T., Williams, P., and Dunley, C. (2001, 2002). Countering Cyber War. NATO review.

Standler, R. B. (1999). Tips for Avoiding Computer Crime. Retrieved March 24, 2006, from the World Wide Web: http://www.rbs2.com/cvict.htm

Standler, R. B. (1999, 2002). Computer Crime. Retrieved March 27, 2006, from the World Wide Web: http://www.rbs2.com/ccrime.htm.

Wikipedia (2006). Retrieved March 27, 2006, from the World Wide Web: http://en.wikipedia.org/wiki/Main_Page

Yale, D. (1997). Crime on the Internet. Retrieved March 27, 2006, from the World Wide Web: http://www.dcyale.com/Law_papers/crime_on_net.html#N_2_