IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP5111

Computer Information Systems Threat Analysis on Security

Yi Li
Department of Management/MIS, College of Business, University of West Florida, Pensacola, Florida 32514, USA, Phone: (850) 474-2501, Email: ly1@students.uwf.edu

June Wei
Department of Management/MIS, College of Business, University of West Florida, Pensacola, Florida 32514, USA, Phone: (850) 474-2771, Fax: (850) 474-2314, Email: jwei@uwf.edu

ABSTRACT

The threat from computer and information crime continues unabated and the financial toll is mounting. Despite the continued efforts of government and industry on investment and technology of computer and information security, both the number of instances and the resulting financial losses of computer and information security related to crimes continue to increase at a quadratic rate. This study analyzes the current state of threats to computer and information security and projects their future trend. Time series analysis is used to predict the internet-related attacks and other major attacks. The paper also makes correlation analysis on the number of attacks and their resulting financial losses. The objective of this research is to provide a big picture to help information technology and system staffs, information systems executives and vice presidents, information systems and technology directors, managers and supervisors in business and government to better understand the computer information security threats so that they can make better decisions on how to cope with these threats. It also helps information security technology providers in industry and general computer users to better assess the potential security market by providing a big picture on the state of computer and information security problems to be addressed.

1. INTRODUCTION

The 2003 CSI/FBI survey on computer security in America reveals an alarming fact that the computers are not as safe to use as people generally believe. The computer and information security breaches have been a serious threat to the IT industry (Straub, 1998, McClure, 2001)). This threat affects directly to a dramatically finical losses (Brancheau, et. al, 1996; Taz, 2001). The numbers of attacks and the resulting financial losses have increased continually from 1997 to 2003 (Power, 2003). The 2002 Computer Security Institute/Federal Bureau of Investigation (CSI/FBI) survey on Computer Crime and Security survey reveal that about 90 percent of the survey's respondents, most of which are from large corporations, detected computer security breaches within the last 12 months. And 80 percent of respondents acknowledged financial losses resulting from computer security breaches. Forty five percent respondents were willing and able to quantify their financial loss. The financial losses for these respondents in 2002 increased to $455,848,000 from $377,828,700 in 2001. The actual amount of loss is even bigger because many victims were not willing or able to quantify their loss. For many reasons such as negative publicity, many organizations chose not to report or acknowledge attack or financial loss (Power, 2003). In addition, the annual amount of loss shows an increasing trend since 1997 (Power, 2003).

The financial losses for the U.S economy as a whole are more scaring. In 1997, the U.S. economy suffered a loss of $100 billion due to security breaches (Power, 2002), a loss five times that of 1992. The amount of loss in 1997 already exceeded the gross domestic product (GDP) for many countries (Udelson, 2000). The threat from computer and information crime continues unabated (Whitman, 2003); therefore, managers need to become more informed of the potential alarms for security breaches (Loch and Warkentin, 1992).

In order to make sound decisions in fighting against the attack, the management needs to understand the current state and future trend of their enemy, namely the attacks on information security. Some research has already been done in the security area. Whitman (2003) and Wood (2000) made in-depth analyses of security. However, they focused more on formulating and implementing a consistent and effective security policy rather than a trend analysis of the threats themselves. In data analysis, they mainly used data collected within 1 year.

This paper is the first attempt in studying the attack patterns of the information security breaches and forecasting their future. It focuses on the trend analysis of security attacks and projects the future of the attacks.

2. METHODOLOGY

All the data in this study is extracted from "Computer Crime and Security Survey", a project conducted by Computer Security Institute (CSI) (Power, 2002; 2003). The Survey can be obtained at the web site http://www.gocsi.com. Established in 1974, CSI is considered the most prestigious international membership organization in information security. CSI has thousands of members worldwide and provides information to assist professionals in information security (Power, 2002).

Attack types studied in this surveyed include denial of service, laptop, active wiretap, telecom fraud, unauthorized access by insiders, virus, financial fraud, insider abuse of net access, system penetration, telecom eavesdropping, sabotage and theft of proprietary information.

Time series analysis is a widely employed forecasting methodology, with application in research of many fields, especially in the forecasting of economic studies, such as price of commodities and financial assets, inflation and gross domestic product (GDP). For instance, this methodology is used for the projection of the weekly live cattle price and the model is found superior to other models (Kenneth and Havenner, 1995). In examining the one-step-ahead forecasts made by USDA on the production of beef, pork and broilers, Sanders and Manfredo constructed an uni-variate time-series model to compare with the USDA forecast and found this simple time series model was more efficient and encompassed more information than the USDA forecast (Sanders and Manfredo, 2002). Time series analysis is also found to have less forecasting error than other methods in projecting the inflation rate (Hafer and Hein, 1990). This methodology is also used in forecasting of GDP of Taiwan (Shen, 1996).

There is still few time series analysis in the study of IT security. In this paper, time series analysis techniques are utilized to forecast the security attack. For all data set, four time series models are used to analyze data, including the Linear Trend Model, the Quadratic Trend Model, the Exponential Trend Model, and the S-Curve Trend Model (Yaffee, 2000).

Correlation analysis is used to study the relationship between the number of incidence of a certain type attack and the average cost of this attack type.

Table 1: Shares of Types of Attack

Year	1997	1998	1999	2000	2001	2002	2003
Denial of Service	6.3%		6.8%	6.5%	8.0%	10.2%	10.0%
Laptop	15.3%	17.6%	15.1%	14.5%	14.2%	14.0%	14.1%
Active Wiretap	0.8%	0.3%	0.4%	0.2%	0.4%	0.3%	0.2%
Telecom Fraud	7.1%	4.4%	3.7%	2.7%	2.2%	2.3%	2.4%
Unauthorized Access of Insider	10.6%	12.1%	12.2%	17.1%	10.8%	9.7%	10.8%
Virus	21.6%	22.9%	19.7%	20.5%	20.8%	21.7%	19.6%
Financial Fraud	3.2%	3.9%	3.1%	2.7%	2.7%	3.1%	3.6%
Net Abuse	17.9%	21.2%	21.2%	19.1%	20.1%	19.9%	19.1%
System Penetration	5.3%	6.3%	6.6%	6.0%	8.8%	10.2%	8.6%
Telecom Eavesdropping	2.9%	2.5%	3.1%	1.7%	2.2%	1.5%	1.4%
Sabotage	3.7%	3.9%	2.8%	4.1%	4.0%	2.0%	5.0%
Theft of Proprietary info	5.3%	5.0%	5.5%	4.8%	5.8%	5.1%	5.0%

3. FINDINGS

This section conducts trend analysis on the frequency of different types of attack with data collected from 1997 to 2003. It also discusses the forecasting on different types of attacks with time series analysis.

In time series forecasting, for most data set, the result shows that Quadratic Trend Model fits better than S-Curve Trend Model, Linear Trend Model or Exponential Trend Model, based on the comparison study for MAPE, MAD and MSD values (Yaffee, 2000).

3.1 Type of attacks on computer systems

The data of one type of attack is measured by the percentage of the total survey participants. This data reflects the percentage of respondents' acknowledgement of this attack occurrence for that particular year. The data is processed into share data. The share of one attack type for a year is defined as the percentage of the data of this attack type in relation to the sum of the data of all attack types for that particular year. Table 1 presents the share of 11 types of attacks on computer security from 1997-2003.

The growth pattern of different types of attack varies from one to another. A few types of attack, such as denial of service, increase quite sharp and continuously. Most types of attack present a downward pattern. Among them are some types of attack which account for a significant portion of all attacks. They include virus, laptop, and unauthorized access by inside users and inside abuse of net access. The table also shows other major trends:

- Virus maintains the top position among all types of attack for almost six years except 1999. In 2003, its share reaches about 19.6. However, this attack did not display a sharp increasing trend. Across the seven years from 1997 to 2003, the variance of data on virus attack is relatively small. In the meantime, the share of attack by virus decreased from 21.6 percent in the base year. Viruses have been a traditional threat to computer security. Therefore, the managers for information security have maintained a steady emphasis on the protection against viruses. This may explain the growth pattern of attack by virus.
- Inside abuse of net access, laptop and unauthorized access by insiders follows virus as the top threats to security. In 2003, they were ranked as the second, third and fourth frequent attacks.
- Denial of service and system penetration are two emerging major threats. They are ranked in fifth and sixth position in 2003 while in 1998 they took the sixth and seventh positions respectively. In 1998, denial of service accounted for 6.3 percent of all attacks. In 2003, its share increased to 10.0 percent of all attacks. The share of system penetration also rose dramatically since 1998. In 2003, it increased to 8.6 percent from 5.2 percent in 1998. Both of the two types of attack mainly come from internet connection. This supports the hypothesis that internet-related attacks increased significantly in the six years from 1998 to 2003.
- Active wiretap remains the least frequent attack.
- In 2003, the top six threats are virus, inside abuse of net access, laptop and authorized access by insiders, denial of service and system penetration. They accounted for 19.6, 19.1, 14.1, 10.7, 10.0 and 8.6 percent of all attacks respectively.
- In terms of their share, all attacks can be basically classified into four groups. The first group includes virus, inside abuse of net access, laptop and authorized access by insiders. Their shares in 2003 are 19.6, 19.1, 14.1 and 10.7 percent. Denial of service and system penetration are in group two, and their shares are 10.0 and 8.6 percent in 2003. They present a continuous and sharp increase pattern in the six years. The third group includes the remaining types except active wiretap. Active wiretap is the last group with only 0.2 percent in 2003.

3.2 Forecasting on types of attack

For all types of attack, the Quadratic Trend Model of time series analysis is selected as the best model and used to project growth of attacks. The residual analysis from the best models shows random patterns.

Table 2 presents the projected data of each type of attack from 2004 to 2006. The table also shows the indices of these data with the value 2003 as the base year. These data are projected by the best fit models. In Table 2, some trends can be identified:

- By 2006 most types of attack will decrease, although a few types will increase until that year.
- Virus will still be the largest threat and will account for 19 percent of all attacks. However, it will show a significant decreasing trend.
- Denial of service will rise from the fifth position in 2003 to the second position in 2006. It will account for 18.6 percent of all attack.
- System penetration will be another rising star and will rise to the fourth position in 2006 from the sixth position in 2003. This attack will account for 11.3 percent of all attacks.
- Inside abuse of net access will have the largest proportion of decrease. However, it will still account for 11.1 percent of all attacks.
- By 2006, the top four attacks will be virus, denial of service, system penetration and laptop. Laptop will account for 11.6 percent of all attacks.
- Active wiretap and telecom eavesdropping will still be the attacks with the least share among all attacks in 2006. Both of their shares are below 1 percent.
- By 2006, the arithmetic sum of the data of all types of attack will decrease to 314 in 2006 from 418 in 2003. However, this does not necessarily indicate a reduction in overall threat. New types of threat may emerge and are not included in this forecasting.

3.3 Correlation between attacks and their cost

This paper also studies the correlation between the number of attacks of a certain type that causes financial losses and the amount of financial losses of this type of attack. The number of attacks is measured by the number of respondents who acknowledged financial losses. Average loss per respondent caused by each type of attacks represents the amount of financial losses. The correlation analysis shows some

Table 2: Forecast Values and Shares of Attack Types

Year	2004		2005		2006	
	Forecasting Values	Shares	Forecasting Values	Shares	Forecasting Values	Shares
Denial of Service	47.6	12.4%	52.9	15.0%	58.6	18.6%
Laptop	50.7	13.3%	44.2	12.5%	36.4	11.6%
Active Wiretap	1.3	0.3%	1.5	0.4%	1.8	0.6%
Telecom Fraud	12.6	3.3%	16.4	4.7%	21.7	6.9%
Unauthorized Access of Insider	32.6	8.5%	22.8	6.5%	10.9	3.5%
Virus	76.7	20.0%	69.3	19.7%	60.1	19.1%
Financial Fraud	15.1	3.9%	16.6	4.7%	18.5	5.9%
Net Abuse	66	17.3%	52.1	14.8%	35	11.1%
System Penetration	38.4	10.0%	37.4	10.6%	35.4	11.3%
Telecom Eavesdropping	4.1	1.1%	2.4	0.7%	0.4	0.1%
Sabotage	19	5.0%	21	6.0%	23.3	7.4%
Theft of Proprietary info	18.6	4.9%	15.9	4.5%	12.5	4.0%
Sum	382.6		352.4		314.6	

attacks types are more correlated to their costs than other types are. According to the correlation coefficient, all types of attacks can be grouped as the following:

- Virus shows a strong positive correlation of 0.76. The data shows that as the number of virus attack increases, the average loss caused by this attack also increase quite proportionally.
- Medium positive correlation includes denial of service (0.47), unauthorized access (0.44), net abuse (0.59) and sabotage (0.67).
- System penetration and theft of proprietary information show weak positive correlation. Their correlation coefficient is 0.18 and 0.14 respectively. The data for theft of proprietary information shows that while the number of this attack type stays at a similar level, its average cost increases at a quicker pace. This indicates each incidence of this attack costs more on the victims.
- Strong negative correlation includes financial fraud (-0.76). The year 2001 and 2002 see the least number of this attack type. However, it is also in the same years that this attack type causes the most losses. This may stem from the same reason as that for the theft of proprietary information, each incidence cost much more.
- Medium negative correlation includes laptop (-0.35).

4. DISCUSSIONS AND CONCLUSIONS

There are three major findings in this paper.

First, the attack as a whole followed a wave pattern trend. Virus remained as the top threat for almost 6 years. In 2003, it accounted for about 19.6 percent of all attacks. However, this attack did not display a sharp increasing trend. Its data in 2003 is about the same as those in the base year. In the meantime, its share in all attacks decreased from 21.6 percent in the base year. As the earliest and the most usual attack type, virus has received attention from security professional for a long time. Many prevention technologies and security procedures have been developed to fight viruses. The data may imply that viruses have been under control to a certain extent. Denial of services and system penetration are two emerging major threats. Their ranking rose from sixth and seventh position in 1998 to fifth and sixth position in 2003 respectively. In 1998, denial of service accounted for 6.3 percent of all attacks. In 2003, its share jumps to 10.7 percent. Share of system penetration rose dramatically from 5.2 percent in 1998 to 8.6 percent in 2003. In 2003, the top 6 threats are virus, inside abuse of net access, laptop, unauthorized access by insiders, denial of service and system penetration. They account for 19.6, 19.1, 14.1, 10.7, 10.0 and 8.6 of all attacks respectively.

Second, this paper also makes forecasts on the attacks for the period from 2004 to 2006 using time series analysis. The Quadratic Trend Model is selected as the best fit model and used to project the growth of attacks. The forecast shows that the data for most attack types will follow a decreasing trend while a few will increase. Virus will still be the largest threat and will account for 19 percent of all attacks. However, it will show a significant decreasing trend. Although the attacks will decrease as a whole, a few attack types will increase dramatically. Denial of service and system penetrations will be very important attack types. By 2006, denial of service will become the second largest threat, only next to virus, while in 2003 it is ranked only the fifth. This attack will account for 18.5 percent of all attacks in 2006. System penetration will be fourth largest attack and will account for 11.2 percent of all attacks. By 2006, the top five attacks will be virus, denial of service, unauthorized access of insider, system penetration and laptop. Unauthorized access and laptop will account for 3.46 and 11.58 percent of all attacks respectively.

Finally, different attack types show different level of correlation between the attacks and their cost. Virus attack shows the most strong positive correlation, and denial of service, unauthorized access, net abuse, and sabotage the medium positive correlation. Financial fraud displays a strong negative correlation. The negative correlation may indicate that each attack costs more on victim.

5. CAVEATS AND LIMITATIONS

Although the data covers a nation-wide sample and is collected by highly regarded institution, the result of the research should still be interpreted with a number of limitations in mind. First, the data set extracted contained information only from persons who responded to the survey. As with all survey data collected, non-response rate might be a problem. Second, there are some important factors affecting the forecasting of attacks. Some of them might be random factors, including the emerging of new attack types and the changes in legal environments:

- Technology factor: This paper did not attempt to study whether the types of attack substitute one another. However, when one type of attack appears, it would take some time for the security technology providers to come up with the counter measures. Therefore, it would probably more effective than some long existing type of attack, such as some types of virus already under the control of anti-virus software. Attackers would probably favor the new type of attack over the long existing ones. The readers should take this into consideration.
- Change in legal environment: The impact of changes in the legal environment on information security is obvious. The legislation on the downloading of MP3 music illustrates such impact. The approval of EEA in 1996, which brings about less U.S based security attack, is another good example (Power, 2002).

REFERENCES

Brancheau, J. C, Janz, B. D., and Weatherbe, J.C. (1996). J.C. Key issues in information system managements: 1994-95 SIM Delphi results. *MISQ* .20, 2, 225-242

Loch, K. D., Carr, H. H., and Warkentin, M. E. (1992). M.E. Threats to information systems: Today's reality, yesterday's understanding. *MISQ*.16, 2, 173-186

McClure, D. (2001). Guarding Your Gateway. *Association Management*. 53, 8, 60-6

Power, R. (2002). 2002 CSI/FBI computer crime and security survey. *Computer Security Issues & Trends*. 8, 1, 1-24

Power, R. (2003). 2003 CSI/FBI computer crime and security survey. http://www.gocsi.com/press/20030528.jhtml [September 15, 2003]

Straub, D. W. and Welke, R. J. (1998). Coping with system risk: Security planning models for management decision making. *MISQ*.22, 4, 441-469.

Udelson, T. (2000). HOW SECURE IS YOUR NET WORK?. *Association Management*. 52, 6, 25-6

Whitman, M. (2003). Enemy at the gate: Threats to Information Security. *Communications of the ACM*. 46, 6, 91-95

Wood, C.C. (2000). Integrated approach includes information security. *Security*. 37, 2, 43-44.

Yaffee, Robert (2000). *Introduction To Time Series Analysis And Forecasting With Applications Of SAS And SPSS*. Academic Press.

Foster, Kenneth A., Havenner, Arthur M., Walburger, Allan M. (1995). System Theoretic Time-Series Forecasts of Weekly Live Cattle Prices. *American Journal of Agricultural Economics*. 77, 4, 1012-1023.

Hafer, R. W., Hein, Scott E. (1990). Forecasting Inflation Using Interest-Rate and Time-Series Models: Some International Evidence. *Journal of Business*. 63, 1, 1-17.

Shen, Chung-Hua (1996). Forecasting Macroeconomic Variables Using Data of Different Periodicities. *International Journal of Forecasting*.12, 2, 269-282.

Sanders, Dwight R.; Manfredo, Mark R (2002). USDA Production Forecasts for Pork, Beef, and Broilers: An Evaluation. *Journal of Agricultural and Resource Economics*. 27, 1, 114-127.