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

ITP5114

Forecasting on Information Systems Attack Sources

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

YiLi
Department of Management/MIS, College of Business, University of West Florida, Pensacola, Florida 32514, USA, Phone: (850) 474-2501

ABSTRACT

The stakes involved in information system security have risen. Organization is vulnerable to numerous types of attacks from many different sources. This intrusion results in a devastating impact in terms of lost assets and good will. This paper analyzes the current growing patterns of likely sources of attacks on information systems security based on historical data from 1997 to 2003. The current trend patterns are analyzed using indices and growth rates. The future trend of these sources of attacks is projected using time series analysis method. This research helps people who are interested in information systems security to better understand the likely source of attacks to information systems. The developed projecting models can help people to forecast the future for each of these likely sources of attacks to information systems. It also assists information technology staffs and managers in industry and government to make strategic management decisions on information systems security.

1. INTRODUCTION

The stakes involved in information system security have risen (Pfleeger and Plfeeger, 2003). Organization is vulnerable to numerous types of attacks from many different sources. This intrusion results in a devastating in terms of lost assets and good will (McCarthy, 2003). The likely sources of attacks are foreign government, foreign corporation, hacker, U.S competitors, and disgruntled employee. The financial losses from these likely sources of attacks in 2002 increased to $455,848,000 from $377,828,700 in 2001 (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 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).

Some executives have already come to realize the importance of information security (Wood, 2000; Campbell et al., 2003). In a survey, when European business executives were asked what the biggest barrier for the greater usage of e-commerce was, 66 percent of them answered "security or privacy" (Daughtrey, 2001). However, the information security issue was not addressed sufficiently by the management in the industry. Information security continues to be ignored by managers and employees. IT executives have often considered the information security important but not critical (Straub and Welke, 1998; Whitman, 2003). IT managers tended to believe that they had already sufficiently addressed the problem or that the security issue was not as important as other issues (Whitman, 2003; Brancheau et al, 1996).

1.1 Problems

The estimating and forecasting of sources of attacks can help the IT managers in decision making by informing them what the major attacks are and which types of attacks will pose major threats in the near future. With this understanding, the IT manager can formulate appropriate security strategies, including resource allocation, proper procedure formulation, and technologies acquisition. The vendors that provide security technologies and products also need the information for assessing the current state of the security technologies market and their market positioning.

However, to make a forecast for the source of attack is not an easy task. Ideally the forecasting should be based on data collected from a sample as large and random as possible and accumulated over many years. However, it is hard to determine how large and random is large and random enough. Real large and random sampling is also very difficult to implement. At the same time, information security is a fast changing arena. Yesterday's story may not be repeated in the future, which forms the basic idea for any regression analysis.

1.2 Objectives

In order to make sound decisions in information security strategies and implementation, decision makers in information technology require an overall picture of the computer security breaches.

An important objective of this paper is to analyze the patterns of attacks and project their patterns in the future so as to help people to understand them better. To be specific:

- Help people who are concerned about the security breaches, especially the IT managers, to better understand the current state of the attacks by giving them a large picture of the attacks. Project the future development of the attacks to help them to decide the prevention strategy.
- Provide data and analysis for researchers to analyze the results of the estimates and forecasting, and share the data with interested parties both in industry and in academics.
- Assist information technology staffs and managers in industry and government to make strategic management decisions on information systems security.

This paper is the first attempt in forecasting the likely source attack patterns of the information security. It focuses on the current trend analysis of sources of attacks and projects the future of the likely sources of attacks.

2. METHODOLOGY

This study analyzes the growth indices and growth rates of attack sources based on historical survey from 1997 to 2003. Five attack sources were discussed in this paper, including foreign government, foreign corporations, independent hackers, U.S competitors, and disgruntled employees.

Data in this study is extracted from a survey 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). In obtaining most of dataset, CSI collected questionnaires from more than 500 respondents. Some data was collected from more than 600 respondents. Most respondents of the survey work for large corporations. They concentrated in high-tech, financial services and manufacturing. The rest are from federal or local government agencies. Index is used for assessing the long-term behavior of the data set since this mathematical tool allows the use of a base year for assessing longitudinal changes. In this study, the base year selected is 1997, if the data is available that year.

Growth rate is defined as the percentage of the difference between the data of the current year and that of the previous year, divided by the data of the previous year. Growth rate is used to evaluate the short-term behavior that is inherent in the data set. Major fluctuations between immediate periods observed can easily be detected using this simple mathematical tool. Time series analysis techniques are utilized to forecast the security attack and technology. 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).

3. FINDINGS

This section conducts trend analysis on the source of security attack and the frequency of different types of attack with data collected from 1997 to 2003. Indices and growth rate methods are employed in this analysis. This section also discusses the forecasting on attack sources and 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 Likely source of attack

The data of one attack source is the percentage of respondents who believed this source to be a likely source of attack. The share of one attack source for a year, or the percentage of the data of this attack in relation to the sum of all likely attack sources for that particular year, are presented in Table 1. Some major findings in this table include:

- Hackers become the largest source of attack in 2003, while in 1997 the top attack source was the disgruntled employee. The share of hackers increases to 32.5 percent in 2003 from 28.5 percent in 1997. In fact, after 2001, hacker replaced disgruntled employee as the largest source of attack. With the penetration of Internet into American society and economy, hackers gained access to attack more American targets. Every person or organization "online" faces the threat from a hacker in another corner of the world. Also, hackers could attack U.S targets on behalf of other sources of attack, such as foreign Corporations or foreign governments (Power, 2002).
- Foreign government is also an emerging attack source. Although it remained as the least attack source in most years, its share in attack source increased from 8.6 percent in 1997 to 11.1 percent in 2003. In 2003, it exceeded foreign corporation and is no longer the least attack source.

Table 1: Share of Likely Source of Attack

Year	1997	1998	1999	2000	2001	2002	2003
Foreign Government	8.6%	8.1%	8.0%	8.4%	9.5%	10.5%	11.1%
Foreign Corp	9.0%	11.2%	11.4%	10.4%	11.8%	10.5%	9.9%
Hacker	28.5%	27.8%	28.0%	30.9%	30.9%	33.2%	32.5%
U.S competitors	19.9%	18.5%	20.1%	17.7%	18.7%	15.4%	15.9%
Disgruntled Employee	34.0%	34.4%	32.6%	32.5%	29.0%	30.4%	30.6%

Table 2: Indices of Likely Source of Attack

Year	1997	1998	1999	2000	2001	2002	2003
Foreign Government	100.0	95.5	95.5	95.5	113.6	118.2	118.2
Foreign Corp	100.0	126.1	130.4	113.0	134.8	113.0	113.0
Hacker	100.0	98.6	101.4	105.5	111.0	112.3	112.3
U.S competitors	100.0	94.1	103.9	86.3	96.1	74.5	74.5
Disgruntled Employee	100.0	102.3	98.9	93.1	87.4	86.2	86.2
Average	100.0	103.3	106.0	98.7	108.6	100.9	100.9
Max	100.0	126.1	130.4	113.0	134.8	118.2	118.2

- Disgruntled employee remained as a major attack source from 1997 to 2003. However, its share decreases to 30.6 percent in 2003 from 34.0 percent in 1997.
- American competitors followed a similar pattern as disgruntled employee. In 2003, its share decreased to 15.9 percent from 19.9 percent in 1997. The approval of Economic Espionage Act (EEA) in 1996 may explain the U.S based attacks, mainly from U.S competitors and disgruntled employee, are deterred to a significant extent. (Power, 2002).
- Foreign Corporation remained as a steady attack source. Its share was 9.0 percent in 1997 and 9.9 percent in 2003.
- In 2003, attack sources and their shares are: hackers, 32.5 percent; disgruntled employees, 30.6 percent; U.S competitors, 15.9 percent, foreign governments, 11.1 percent; foreign corporations, 9.9 percent.

Data of attack sources are also processed into indices and are presented in table 2.

Table 2 reveals the following information:

- Index of foreign government in 2003 reaches 118.2, the highest among all attack sources.
- In 2003, disgruntled employee index is only 86.2, the second lowest index.
- U.S competitors have an index of only 74.5, the least index in 2003.

Table 3 presents the growth rates of the data on attack sources. Growth rate can be used to evaluate the short-term behavior that is inherent in the data set, and observe the major fluctuations between immediate periods.

In Table 3, information revealed includes:

- Hackers have maintained positive growth rates since 1998.
- The growth rate of foreign government has been positive since 1998. It is interesting to notice that foreign government has the largest yearly growth rate among all sources since 2001. This corresponds with the terrorist attack which fundamentally changed the security perception of Americans.
- The growth rate of disgruntled employee remained negative since 1998.

3.2 Forecasting of likely source of attack

Time series forecasting analysis is used to forecast the source of attacks from 2004 to 2006. The best models from time series study and their respective MAPE, MAD and MSD values are presented below. Except hackers, Quadratic Trend Model is selected as the best model and is used to project growth of attack sources. The residual analysis from the best models shows random patterns.

Table 3: Growth Rate of Likely Source of Attack

Year	97-98	98-99	99-00	00-01	01-02	02-03
Foreign Government	-4.5%	0.0%	0.0%	19.0%	4.0%	4.0%
Foreign Corp	26.1%	3.4%	-13.3%	19.2%	-16.1%	-16.1%
Hacker	-1.4%	2.8%	4.1%	5.2%	1.2%	1.2%
U.S competitors	-5.9%	10.4%	-17.0%	11.4%	-22.4%	-22.4%
Disgruntled Employee	2.3%	-3.4%	-5.8%	-6.2%	-1.3%	-1.3%
Average	3.3%	2.7%	-6.4%	9.7%	-6.9%	-6.9%
Max	26.1%	10.4%	4.1%	19.2%	4.0%	4.0%

Foreign Government:	Yt = 22.8571 - 1.5238*t + 0.3333*t**2 MAPE: 2.494, MAD: 0.5850, MSD: 0.5442
Foreign Corp:	Yt = 20.2857 + 4.5119*t - 0.5595*t**2 MAPE: 6.1225, MAD:1.6666, MSD: 3.5034
Hacker:	Yt = 69.8417*(1.0253**t) MAPE: 1.5204, MAD: 1.1694, MSD: 1.6083
U.S competitors:	Yt = 50.4286 + 0.5357*t - 0.3214*t**2 MAPE: 6.1490, MAD: 2.7755, MSD: 9.4489
Disgruntled Employee:	Yt = 92.7143 - 3.3809*t + 0.1190*t**2 MAPE: 2.4670, MAD: 2.0136, MSD: 4.7687

Table 4 presents the forecast values for different types of attack sources. In Table 4, hacker and foreign government will continue to grow as attack sources. Other major trends are identified as follows.

- Hacker will be the leading attack source in 2006. In 2006, its share will increase to 38.3 percent from 32.5 percent in 2003. It will have exceeded disgruntled employee by almost 26.7 percent by that time. In 2003, it is only 6.5 percent more than disgruntled employee.
- Foreign government will continue to grow sharply as an attack source. In 2006, its share will increase to 17.5 percent from 11.1 percent in 2003. In 2003, it is only 8 percent more than foreign corporations. In 2006, it will be 333.2 percent higher than foreign government.
- Disgruntled employee still takes a big share of 30.3 percent. The internal control is always a difficult problem to deal with.

4. CONCLUSIONS

Attacks on compute and information security have become major issues in information technologies since they caused tremendous losses and posed severe threats to the normal functioning of information systems. Although a lot of research has been done in information security, this paper is the first attempt to analyze the trend of attack sources and forecast the future of them with time series methodology.

The results of this research can assist decision makers in information technology, including computer information system users, security technology providers, and information systems managers, to make strategic management decisions on information systems attacks. These people need to have a good understanding of attacks on information security so that they can make sound decision regarding how to protect their information and systems or assessing what security technologies the market will need. Specifically, the results of this research assist information technology staffs and managers in industry and government to make strategic management decisions on information systems security; help people who are interested in information systems security to better understand the likely source of attacks to information systems; and forecast the future for each of these likely sources of attacks to information systems.

This paper provides a big picture of both the current and future trends on different sources of attacks on information systems, with a focus on the analysis of evolvement patterns of information security attack sources and the projection of its future trend. In analyzing the attack patterns, mathematical tools such as index and growth rate method are utilized. In projecting the future trend, time series analysis is employed.

Table 4: Forecast of Attack Source of Shares

Year	2004		2005		2006	
	Forecasting Values	Shares	Forecasting Values	Shares	Forecasting Values	Shares
Foreign Government	32	13.0%	36.1	15.0%	41	17.5%
Foreign Corp	20.6	8.4%	15.6	6.5%	9.5	4.0%
Hacker	85.3	34.8%	87.4	36.4%	89.7	38.2%
U.S competitors	34.1	13.9%	29.2	12.2%	23.6	10.1%
Disgruntled Employee	73.3	29.9%	71.9	29.9%	70.8	30.2%
Sum	245.3		240.2		234.6	

The analysis on attack source reveals that hacker and foreign government are increasingly important attack sources from 1997 to 2003. In 2003, hacker is the largest attack source and has a share of 32.5 percent. It surpassed disgruntled employee and remained as the top attack source since 2001. In 2003, foreign government exceeds foreign corporation and has a share of 11.1 percent. Disgruntled employee continues to hold a major share although it showed a decreasing trend. In 2003, it is the second largest attack source and has a share of 30.6 percent. September 11 causes people to worry about the threat from abroad. Some foreign governments have the resources and technology to conduct organized attacks. The expansion of the Internet and the high internet penetration rate empower hackers from abroad and gives them access to more U.S targets. With the increasing law enforcement and legislation against computer crime in America, U.S based attacks reduced. The paper also projects attack source from 2004 to 2006. The forecasting shows that hacker will continue to grow sharply. It will remain as the top attack source from 2004. Hacker will surpass disgruntled employ by 26.7 percent and will have a share of more than 38 percent by 2006. Although disgruntled employee will decrease, it will still hold a considerable share of 30.1 percent.

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 attack sources and attacks. Some of them might be random factors, including the emerging of new attack sources and the changes in legal and political environments:

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. *MIS Q* .20, 2, 225-242

Daughtrey, T. (2001). Costs of Trust for E-Business. *Quality Progress.* 34 no10 38-43 O

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.

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.

Pfleeger, C. P., and Pfleeger, S. L. (2003). *Security in Computing*. 3rd edition. NJ: Prentice Hall

McCarthy, L. (2003). IT Security: *Risking the Corporation*. 2nd edition. NJ: Prentice Hall

Campbell, P., Calvert, B., and Boswell, S. (2003). Security+. 1st edition. MA: Thomason Course Technology