Assessing Damages of Information Security Incidents and Selecting Control Measures, a Case Study Approach

Fariborz Farahmand, Shamkant B. Navathe, Gunter P. Sharp, Philip H. Enslow
Georgia Institute of Technology

Abstract

Information security executives have always been faced with the problem of justifying security technology investments because the technology benefits are difficult to estimate. There are tangible and intangible benefits that accrue from implementation of security measures; similarly the losses due to security incidents fall into both of these categories. This further complicates estimation. Currently a formal approach to assess damages to information security systems does not exist, neither does a model to select control measures. This paper provides a real world study of the threats to information systems, their damages, and maps some control measures to the threats that can cause these damages.

1. Introduction

Security of information systems is being highly challenged by the recent proliferation of internet-based applications including electronic commerce and a variety of information brokering services. It is imperative that security of an information system should, by design, protect the confidentiality, integrity, and availability of the system. Given the information-intensive characteristics of the modern global economy dominated by the Internet and the World Wide Web, it should be no surprise to learn that information security is a growing spending priority among most companies and government agencies. This growth in spending is occurring in a variety of areas, including software to detect viruses, firewalls, sophisticated encryption techniques, intrusion detection systems, automated data back up, and hardware devices [CERT 2004]. However, studies by the Computer Security Institute and Federal Bureau of Investigation reported that approximately 90% of respondent organizations in 2001 and 2002 detected computer security breaches [Powe 2002]. Moreover, these studies found that the losses averaged over 2 million dollars per organization. In contrast, companies only spend 0.047 percent of their revenues on security [Geer 2003], and this indicates that many firms are not adequately investing in information security. Literature review indicates a large stream of research that focuses on the technical defenses (e.g., encryption, access control, intrusion detection, and firewalls) associated with protecting information [Ande 1972, Denn 1987, Sand 1996, Dani 1999, Schn 1996.] However, there is little comprehensive research on how organizations should:

- Assess the damages of past security incidents.
- Evaluate their present vulnerability (risk) to security incidents.
- Prepare for facing security incidents by selecting appropriate control measures given the resource constraints of finances, manpower, and software tools.
- Train security personnel in law enforcement agencies to better prepare for dealing with security incidents.

In general, research that focuses on the economic aspects of control measures for information security is sparse. Because of the paucity of the work in this area, there is little general guidance to organizations and government agencies on these matters.

1.1- Costs Resulting from Information Security Incidents

A physical breach of security involves actual damage to or loss of the computer hardware or media on which data are stored. A logical breach affects the data and software without physically affecting the hardware. Literature review reveals a stream of research on the cost of information systems security incidents [Ande 2001, Butl 2002, Cohe 1991, Dobs 1994, Orla 1991, Tarr 1995]. One of the problems with any logical breach of security is that the damage is invisible and its extent is unknown. This causes serious difficulties for managers to justify their investments on security. A simple approach for finding return on investment is calculating:

[(Change in revenue) + Cost saving)] / [(Investment)]

However, these parameters are hard to determine. Decisions about return on security investment will not start to make sense until one can replace these parameters with numbers. Literature review has suggested that, by theoretical means, one can demonstrate that the optimal level of investment in security-related activities should not exceed approximately one third of the potential expected loss [Gord 2002]. It is also argued that a cost effectiveness analysis is the preferred analysis method when costs and benefits are not commensurate [ISO 1989, Orla 1989]. Effectiveness is easier to apply because it does not ask the price of events. Instead, it asks, "What is the most one can get for $X, given that one is inevitably going to spend $X?" In other words, it is about maximizing the effectiveness of an expense in pursuit of a benefit not easily valued. Although this approach is not the solution to analysis of investment on security and a replacement for traditional cost benefit approach, it directs security mangers in the right directions.

The literature review also reveals a school of thought that promises economic reasoning and analysis as a solution to security issues of information systems [Blak 2001, Schn 2002]. For example, the success of firewalls is not because of their effectiveness, but because auditors started demanding firewalls and this fact could change the cost equations for businesses. The cost of adding a firewall incurred expense and user annoyance, but the cost of not having a firewall was failing an audit. This reasoning explains that monetizing security can solve business and technical problems for the information security industry. It provides information about both losses and product effectiveness, which are the prerequisites for the formation of a viable security market.

2. Our Approach

We conducted personal interviews with law enforcement agencies dealing with computer crime and with executives from financial institutions dealing with security issues. In addition, we did a literature review of cases prosecuted by the Department of Justice including the evaluation of damages and financial awards [Fara 2003]. This review shows a significant negative market reaction to information security breaches involving unauthorized access to confidential data, but no significant market reaction when the breach does not involve access to confidential data [Camp 2003]. This finding is actually consistent with the findings from the 2002 CSI/FBI Survey, which suggests that among information security breaches, the most serious financial losses were related to theft of proprietary information. This is also consistent with the recently prosecuted computer cases by the Computer Crime and Intellectual Property Section, CCIPS, of the Criminal Division of the U.S. Department of Justice. According to CCIPS, 91% of the cases that have been prosecuted under the computer crime statute, 18 U.S.C. 1030, are the cases related to the violation of confidentiality of information. As an example of these cases, in November 2001, two former Cisco Systems, Inc., accountants were sentenced to 34 months in prison for illegally issuing almost $8 million in Cisco stock to themselves. We sorted the information provided by the 2003 CSI/FBI Survey according to the percentage of detected attacks by respondents, and mapped these attacks into a three dimensional model as shown in Table 1 in the Appendix.

These findings reveal that breaches involving unauthorized access to confidential information are quite different from attacks that do not involve access to confidential information. Once confidential information has been accessed in an unauthorized manner, the value of such a strategic asset may be permanently compromised. For example, a firm's customer list may be an important proprietary asset. Once this list has been accessed without authorization, others may be able to use the list for marketing and other purposes. This may permanently impair the list's value to the firm that created it. In the cases of breaches that do not involve unauthorized access to confidential information, the underlying assets generally relate to operations.

This research also tried to investigate the long-term impact of the announcement of a security breach on firms by comparing the stock value of the victimized firms with their industry indexes. A sample of eight companies: Boeing, First Data Corp, McGraw- Hill, Yahoo, Ebay, Egghead, Raytheon, and Northwest Airlines, who had suffered from a publicized security breach, were chosen. The stock values of these companies, on the day of the incident (t=0), and t+ or - two days, 7 days, one month, one quarter, two quarters, three quarters, and four quarters, (i.e., before and after the incident), were recorded from the Standards and Poor's publications [S & P 1999, 2000, 2001, 2002]. These numbers were also compared with the trend of their related industries in that period of time. We concluded that one cannot draw a definite conclusion about the impact of public announcement of security breaches on firms in terms of their capitalization or market value.

3. Case Studies: Round I

At this stage of our research, the accuracy of findings from the literature review and analysis about the source, classification, and importance of threats to information systems and assigning effective control measures to confront these threats was evaluated by experts [Fara 2004]. Through meetings, telephone conversations, and e-mails, major threats to information assets of companies and to their associated industries in general were discussed. The research was done in four steps:

1. Identifying sources of information.
2. Developing the questionnaire.

3. Analyzing/evaluating the usefulness of answers.
4. Testing and confirming the results in the second round.

Six information security experts participated in these case studies. They were from: 1- A consumer advertising service, 2- A law enforcement agency, 3- An information security consulting service, 4- A network service provider, 5- An online payment service, and 6- An educational service auditor. Four experts participated in round one and two experts, who had contributed in round one, as well as one additional expert, participated in round two. The list of questions of the first round is in the Appendix.

3-1. Summary of the Answers in the First Round

The following summarizes answers in the first round:

- All the respondents listed disclosure and theft of proprietary information as a major threat.
- Virus, Denial of Service (DoS), disgruntled employees, improper password security, hardware failures were also mentioned as threats.
- None to one major attack per month and average of one intrusion every six months.
- All the respondents said they expect at least one major attack during the coming twelve to twenty four months,
- The damage of such an attack would first depend on publicity of the attack, and second on costs of system downtime, notification, consulting, and re-design.
- Unauthorized users were identified as the source of the most important threats to an organization that can be caused by software techniques.
- Most respondents could not describe what exact control measure they had in place. Some listed scanners for viruses, and passwords, firewalls, IDS systems for break-ins.
- Background checks were mentioned as a control measure that is not included in our model.
- All respondents mentioned access control as the most effective control measure for a threat. Respondents were not able to evaluate the effectiveness of the control measures, except for one respondent who estimated 70% effectiveness as an overall effectiveness for the control measures.
- All respondents reported dissatisfaction of users on using passwords and authentication.
- All respondents emphasized the need for a formal methodology in evaluating intangible damages. Only one respondent provided an approach for evaluating damages to reputation.
- Although most of the respondents were interested in transferring risks to insurance companies, they had concerns about issues such as: lack of formal methods for damage assessment, deductibles, covered items, and above all, confusing policies.

4. Case Studies: Round II

In the second round we asked the following questions to expand on and to verify the responses given in round one.

4-1. Questions in Round Two and Summary of the Results

In our first round of interviews with information security experts, we found the following as the top 3 important threats to information assets (ranked in order of importance):

1- Theft of proprietary/ disclosure of information

2- Virus

3- Denial of service attacks

1- Do you agree with this order? If not, what order do you suggest?

2- Do you agree that a company may experience these attacks as follows?

Theft of proprietary/ disclosure of information: Rarely to once a year

Virus: Once every 3 months

Denial of service: Once a year

3- Do you agree with the following control measures for these threats and their effectiveness?

For theft of proprietary/ disclosure of information threats control measures can be listed as:

Perimeter router

Multiple intrusion detection systems

Access control

Firewall

System Log

For virus:

Access control

Virus scanners

For Denial of Service attacks:

Access Control

Firewall

Proactive methods such as application software

If so, what is the effectiveness of these control measures? What other control measure(s) do you suggest for these threats and what do you estimate the effectiveness of this control measure?

All of the respondents agreed with the following ranking of threats in the order of importance:

1- Theft of proprietary/ disclosure of information

2- Virus/worm attacks

3- Denial of service attacks

One expert said:

> *"I agree, number one could be very costly to a business, while two and three can be managed to a degree"*

All of the respondents said that frequency of theft of proprietary information, or disclosure of information, was estimated to be more than just once a year. It was also stated that under several circumstances most of these attacks did not receive publicity. Virus attacks are expected by respondents on a daily basis.

The following is a sample comment by one expert:

> *"I think you are correct in your response, only because this is about how often the above incidents are reported. The first incident is very rarely reported, while the second is known due to the publicity that is reported throughout the industry. As to a DoS attack, with better security and equipment, we don't hear from the victims as much as we used to. This may also be due to the fact that Internet providers are more proactive in stopping DoS attacks"*

The following control measures were approved as effective control measures:

For the theft of proprietary/ disclosure of information threat:

Perimeter router

Multiple intrusion detection systems (IDS)

Access control

Firewall

System Log

(Encryption, IDS, separation of duties, and web content filtering were also suggested by some respondents.)

For virus:

Access control

Virus scanner

(Inline IDS was also recommended.)

For denial of service:

Access control

Firewall

Proactive methods such as application software

(Application firewall running alongside the perimeter routers, border routers, and bandwidth shapers were also suggested by some respondents.)

The following is a sample comment by one expert regarding selecting the effective control measures:

> *"I agree 100 percent; the stronger the control measures, the more dissatisfied the client. People are very impatient, and their time is very valuable. Client's days are very busy and complicated, and in order to generate a good work product, they cannot be frustrated by security controls that have been put in place. Installing complicated security measures, slows down the system, and distracts the client. As to a reasonable time, I do not know, but we both know the faster the better"*

5. Conclusions and Future Work

The work presented above was based on a case study approach, but we believe that the outcome of this study is sufficient to warrant continued development. In particular, we have identified the order of importance of threats to information systems of organizations as follows:

1- Theft of proprietary/ disclosure of information

2- Virus/worm attacks

3- Denial of service attacks

Respectively, this research identifies perimeter router, multiple intrusion detection systems, access control, firewall, and system logs as control measures for the first threat; access control and virus scanners for the second threat; and finally, access control, firewall, and proactive methods for denial of service attacks.

We also noticed that currently chief information security officers do not know about the effectiveness of existing control measures and do not have any formal method for evaluating their effectiveness. Our previous work [Fara 2003] assigns seven control measures to threats to information systems. Future work would involve choosing the level of control measure, (L). This will be related to the effectiveness (E) and cost (C) of control measures as shown in Table 2 in the Appendix. The values will be estimated by interviewing security managers. Ultimately, the results will be used in our five-stage risk analysis system [Fara 2004].

Another area of future research is a tradeoff analysis between the costs of security measures and the incident rate, where the latter is a proxy measure of system reliability. A multi-objective optimization approach could be used here to find the Pareto-optimal set of solutions.

Acknowledgment

This paper is based on the results of a research undertaken by the authors at the Georgia Tech College of Computing and the authors would like to express their sincere thanks to Dr. Jean Camp of Indiana and Harvard University and Mr. Bill Malik for their contribution in this research.

References

[Ande 1972] Anderson, J., "Computer Security Technology Planning Study," U.S. Air Force Electronic Systems Division Tech. Rep., Oct. 1972, pp. 51-73.

[Ande 2001] Anderson, R., "Why Information Security is Hard- An Economic Perspective," *17th Annual Computer Security Applications Conference*, Dec. 2001.

[Blak 2001] Blakley, B., McDermott, E., Geer, D., "Information Security is Information Risk Management," *Proceedings of the 2001 Workshop on New Security Paradigms*, 2001, pp. 97-104.

[Butl 2002] Butler, S. A., "Security Attribute Evaluation Method: A Cost-Benefit Approach," *Proceedings of the 24th International Conference on Software Engineering*, ACM, May 2002, pp. 232-240.

[Denn 1987] Denning, D. 1987, "An Intrusion-detection Based Model," *IEEE Transaction Software Engineering*, Vol. 13, No. 2, Feb. 1987, pp. 222-226.

[Camp 2003] Campbell, K., Gordon, L. A., Loeb, M. P., Zhou, L., "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market," *Journal of Computer Security*, Vol. 11, 2003, pp. 431-448.

[CERT 2004] http://www.cert.org

[Cohe 1991] Cohen, F., "A Cost Analysis of Typical Computer Viruses and Defenses," *Computers & Security*, Vol. 10, 1991, pp. 239-250.

[Dani 1999] Daniels, T., E., Spafford, E. H., "Identification of Host Audit to Detect Attacks on Low-level IP," *Journal of Computer Security*, 1999, Sec. 7- 1, pp. 3-35.

[Dobs 1994] Dobson, J., "Messages, Communication, Information Security and Value," *Proceeding of the New Security Paradigms Workshop*, IEEE, Aug. 1994, pp. 10-18.

[Fara 2003] Farahmand, F., Navathe, S. B., Sharp Gunter P., Enslow, P. H., "Managing Vulnerabilities of Information Systems to Security Incidents," *ACM ICEC 2003*, Pittsburgh, Sept. 2003.

[Fara 2004] Farahmand, F., *Developing a Risk Management System for Information Systems Security Incidents*, Ph.D. Dissertation, College of Computing, Georgia Institute of Technology, Dec. 2004.

[Geer 2003], Geer, D., Soo Hoo, K., J., Jaquith, A., "Information Security: Why the Future Belongs to Quants," *IEEE Security and Privacy*, 2003, pp. 32-40

[Gord 2002] Gordon L. A., Loeb, M. P., "Return on Information Security Investments," *Strategic Finance*, Nov. 2002.

[ISO 1989] ISO, "Information Processing Systems- Open Systems Interconnection-Basic Reference Model, Part 2: Security Architecture," *ISO 7498-2, 1989.*

[Orla 1989] Orlandi, E., "Computer Security Economics," *ICCST,* 1989, pp. 107-111.

[Orla 1991] Orlandi, E., "The Cost of Security," *Proceeding of the 25th Annual IEEE International Carnahan Conference on Security Technology*, Oct. 1991, pp. 192 –196.

[Powe 2002] Power, R., *Computer Security Issues & Trends, 2002 CSI/FBI Computer Crime and Security Survey*, CSI, Vol. VIII, No. 1.

[S & P 1999-2002] S & P, *Industry Surveys*, Standards and Poor's, McGraw-Hill, 1999, 2000, 2001, and 2002.

[Sand 1996] Sandhu, R. S., Coyne, E., J., Youman, C. E., 1996, "Role-based Administration of Rules," *ACM Transactions of Information Systems*, Sec. 1, 2, Feb. 1999, pp. 105-135.

[Schn 1996] Schneier, B., 1996, *Applied Cryptography,* Wiley, New York, 1996.

[Schn 2002] Schneier, B., "No, We Don't Spend Enough," *Workshop of Economics and Information Security*, May 2002.

[Tarr 1995] Tarr, C.J., "Cost Effective Perimeter Security, Security and Detection," *European Convention on Security and Detection*, 1995, pp. 183-187.

Appendix

Table 1-Security incidents detected in 2003 (reported by FBI/CSI) classified by agent-technique, based on data contained in FBI/CSI Report, and the suggested control measures

Attack	Agent	Threat	% Detected	Security Measure
Virus	Unauthorized	SW	85	Data integrity
Insider abuse of net access	Authorized	SW & Personnel	78	Authentic. & Access control
Laptop theft	Unauthoriz. & Authoriz.	Phys. & Personnel	55	All five measures
Denial of service	Unauthorized	SW	40	Authentic. & Access control
System penetration	Unauthorized	SW & HW	40	Authentic. & Access control
Unauthoriz. insider access	Unauthorized	Personnel	38	Authentic. & Access control
Theft of proprietary information	Unauthoriz. & Authoriz.	SW & Procedural	20	Authentic. & Access control
Financial fraud	Unauthoriz. & Authoriz.	Procedural	12	Authentic. & Access control
Telecom fraud	Unauthorized	SW & HW	9	Authentic. & Access control
Sabotage	Unauthoriz. & Authoriz. & Environmental	HW & Physical	8	Access control
Telecom eavesdropping	Unauthorized	HW	6	Data confidentiality
Active wiretap	Unauthorized	HW	1	Data confid. & Data integrity

Table 2- Threat-control measure relation, effectiveness values by level

		Authentication	Access Control	Data Conf.	Data Integrity	Non Repudiation
Unauthorized User	Software					
	Hardware					
	Procedural					
	Personnel					
	Physical					
Authorized User	Software					
	Hardware					
	Procedural					
	Personnel					
	Physical					
Environmental Factor	Software					
	Hardware					
	Procedural					
	Personnel					
	Physical					

First Round of Interviews

The following are the thirteen questions asked during the first round of four case studies:

Question 1- What do you think would be the most important threat(s) to the information system of your company?
Question 2- How many times have you experienced this type of threat(s)/incident(s) during the last 12 months?
Question 3- If the threat has not yet occurred, how long do you think it will be (in months) before you suffer such a threat?
Question 4- What type of damages did this/these threat(s) cause? (or would likely cause)?
Question 5- Is/are this/these threat(s) more likely to be caused by unauthorized or authorized users by using software techniques?
Question 6- What control measure(s) did you have in place that failed to stop the threat?
Question 7- What type of control measure do you use for this/these threat(s) that do not fall in the category of access control, authentication, data confidentiality, data integrity, and non-repudiation services?
Question 8- According to the CSI/FBI Survey, attacks which can cause the most serious financial damages are: theft of propriety information, financial frauds, and viruses. Do you think this/these attack(s) are more likely to be caused by unauthorized or authorized users by using software techniques?
Question 9- Which combination of control measures do you prefer?
Question 10- How would you rate the effectiveness of these control measures? For example, to what degree did this/these control measure(s) reduce the probability of the threat or the actual cost of the damage?
Question 11- In some cases, using stronger control measures can cause dissatisfaction of clients, e.g. using stronger encryptions cause delay in response time. What is the maximum response time to a mouse click, in seconds, that you consider acceptable for your web-based customers?
Question 12- In making financial decisions, do you consider the intangible damages of an incident to your company, e.g. negative impact of announcement of a breach on stock market or on clients? If so, what metrics/evaluation criteria do you use to calculate these costs?
Question 13- Will you consider transferring risks to an insurance company? If so, do you find their policies and coverage reasonable?