Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Quantitative Risk Analysis Step-By-Step

In this paper, the use of a centralized data table containing reference data and estimating techniques for some of the key variables for determining risks and losses will help to present a stronger case for security improvement to management. A discussion of methods for the valuation of tangible and intangible assets will help to quantify the largest information security risk in the U.S., which is theft of proprietary information (Computer Security Institute). Additional focus is placed on important risk areas such as ...

Copyright SANS Institute
Author Retains Full Rights

AD

Quantitative Risk Analysis Step-By-Step

By

Ding Tan
December 2002

GSEC Practical Version 1.4b – Option 1

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Table of Contents

1. Abstract 3
2. Introduction 3
3. Importance of Quantitative Risk Analysis 4
4. Quantitative Risk Analysis Procedure And Calculations 5
5. Assigning Values to Tangible Assets 6
6. Assigning Values to Intangible Assets 7
7. Estimating Potential Threat & Risk 9
8. Estimating The Potential Exposure Factor 11
9. Risk Analysis Data 11
10. Method of Data Interpretation 15
11. Overseas Risks And Threats 16
12. Laptop Security 16
13. Internet Threats / Issues 17
14. Conclusions 18

References 20

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

1. ABSTRACT

80% of the companies that participated in the FBI/CSI survey reported financial losses due to security breaches. However, only 44% could quantify their actual losses (Computer Security Institute). In addition, according to a survey conducted in Britain, only 30% of UK businesses had ever evaluated return on investment for information system security spending (PricewaterhouseCoopers). This paper is designed to give the IT professional and security consultants an overall tool in the planning, formulating, and making of a quantitative risk analysis including all of the key variables for management review. Because of the scarcity of reliable data, diversity in subject matter, lack of well-established methodology, and the unavoidable degree of subjectivity of data, the resulting quantitative risk analysis is a difficult thing to accomplish.

In this paper, the use of a centralized data table containing reference data and estimating techniques for some of the key variables for determining risks and losses will help to present a stronger case for security improvement to management. A discussion of methods for the valuation of tangible and intangible assets will help to quantify the largest information security risk in the U.S., which is theft of proprietary information (Computer Security Institute). Additional focus is placed on important risk areas such as internet security, overseas security concerns, and laptop security. This paper should also help an IT security consultant to obtain new business through the creation of a well-written quantitative risk analysis.

2. INTRODUCTION

According to the FBI/CSI 2002 study, even though 89% of the companies surveyed have firewalls and 60% use intrusion detection systems (IDS), an alarming 40% of those surveyed still detected intrusion from the outside (Computer Security Institute). Does this mean their firewalls and IDS are not very effective against outside attacks? In addition, 90% of those surveyed have anti-virus software. But still, 85% were attacked by worms, virus, and other malicious codes. (Computer Security Institute). Does this mean their anti-virus software is ineffective? The answers to these questions may lie in the fact that the existing IT security systems, and security measures may not be enough to withstand the growing attacks by criminals. A tremendous amount of technical support and capital have to be infused to improve the overall security infrastructure. The main problem becomes, how can we justify the spending to protect our information systems?

The lack of a well-documented cost and benefit analysis of security improvement efforts as part of the risk analysis campaign has contributed to the following issues:

- For security consultants, it is difficult to justify new business from a prospective client when no risk analysis has been done to show the projected payback.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- For the individual company, it is difficult to make improvements in security because no new improvements can be justified without proper financial analyses. Management typically cares very much about the bottom line .
- For the IT systems administrators, it is a vicious cycle of firefighting for security issues when much more effective countermeasure proposals are beyond reach due to the lack of proper financial justification.

The key to justifying spending to improve security is first by means of a risk analysis. Two basic types of risk analysis to consider are quantitative risk analysis and qualitative risk analysis. Quantitative risk analysis attempts to assign independently objective monetary values to the components of the risk assessment and to the assessment of the potential loss. Conversely, a qualitative risk analysis is scenario-based (Miller).

Although a qualitative risk analysis may be easier to do at times; a quantitative risk analysis offers the following distinct advantages:

- More objectivity in its assessment
- More powerful selling tool to management
- Offers direct projection of cost/benefit of proposal
- Can be fine-tuned to meet the needs of specific situations
- Can also be modified to fit the needs of specific industries
- Much less prone to arouse disagreements during management review
- Analysis is often derived from some irrefutable facts

To do a quantitative risk analysis, the value of the potential losses associated with delayed processing or the theft or destruction of property or data needs to be determined. Then the probability of the occurrence of the risk failure needs to be estimated. Finally, the annual loss expectancy is calculated (Miller).

Different risk countermeasure strategies will have different payback or cash flow scenarios. For instance, a security upgrade consisting of a sophisticated firewall system with an expensive network intrusion detection system will potentially have relatively long positive cash flow duration. On the other hand, if we had only spent money on hiring a security consultant to conduct security monitoring and services once a month, any positive work that he had done would have been erased in relatively short period of time.

3. IMPORTANCE OF QUANTITATIVE RISK ANALYSIS

Quantitative risk analysis is typically important in different ways to different people:

To the security consultant:

- Development of new security project proposal management skills
- Potentially lure new business through the use of good quantitative analysis to tap into projects that were previously out of reach

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Having a better marketing and selling tool if previous projects turned out to be inline with predicted ROI (return on investment)
- Broaden existing consulting services by adding on cost-effective, high-ROI security improvement strategies and action plans

To the system administrator:

- Better prioritizing of projects – can set priority based on ROI
- Effective means to manage limited department resources
- Easier to obtain funding from management
- Improved performance metrics for the department due to clearly defined cost & benefit information relating to security projects

To the company's upper management:

- A more standardized means to fund projects
- Less susceptible to issues relating to company politics
- Reduced time requirement for assessing the validity of proposals
- Allows the end results to be tied to the company's financial objectives more quickly

The importance of presenting a quantitative risk analysis in a manner similar to a well-managed engineering capital project cannot be underestimated. Uncertainty, ambiguity, risk, and subjectivity make management nervous about spending money; therefore, it is imperative to present a well-prepared quantitative risk analysis to soothe management's anxiety about the unknown. By doing due diligence to collect enough corroborating data, the chance of success for project approval is greatly increased. The ability to "market" one's technical project is a learned skill indeed.

4. QUANTITATIVE RISK ANALYSIS PROCEDURE AND CALCULATIONS

A. Quantitative Risk Analysis Procedure

The following is a step-by-step breakdown of the quantitative risk analysis.

(a) Conduct a risk assessment and vulnerability study to determine the risk factors.
(b) Based on the top 5 risk factors determined in (a), determine the value of assets under risk. For tangible assets, use the information in Section 5 for guidance. For intangible assets, use the information in Section 6 for guidance.
(c) Determine the historical attitude of the company under assessment in regards to their security practice for reporting loss incidents. Use the data in table 3 to make adjustments of the quantitative estimates for risk analysis.
(d) Estimate the Annualized Rate of Occurrence (ARO) for each risk factor.
(e) Determine the countermeasures required to overcome each risk factor.
(f) Determine the Annualized Loss Expectancy (ALE) for each risk factor. See the calculations for ALE section below for details. Please note that the ARO for the ALE after countermeasure implementation may not always be equal to zero.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

(g) Conduct the safeguard cost/benefit analysis by calculating the difference between the ALE prior to implementing the countermeasure to the ALE after implementing the countermeasures (Urban).
(h) Based on the above analysis in (f) & (g), determine the return on investment using Internal Rate of Return (IRR). For details on IRR, refer to Section 4 B below.
(i) Present the results in a summarized fashion to management for review. The methodology used can be similar to that of typical engineering capital appropriation requests.

B. Quantitative Risk Analysis Calculations

The key variables and equations used for conducting a quantitative risk analysis are shown below (Urban) :

Exposure Factor (EF) = Percentage of asset loss caused by identified threat; ranges from 0 to 100%. See Section 8 for details on how to estimate EF.

Single Loss Expectancy (SLE) = Asset Value x Exposure factor; [1]
1,000,000 @ 20% likelihood = $200,000

Annualized Rate of Occurrence (ARO) = Estimated frequency a threat will occur with in a year and is characterized on an annual basis. A threat occurring once in 10 years has an ARO of 0.1; a threat occurring 10 times in a year has an ARO of 10

Annualized Loss Expectancy (ALE) = Single Loss Expectancy x Annualized Rate of Occurrence. [2]
ALE can sometimes be extrapolated from existing comparable data. See Section 7 for more details.

Safeguard cost/benefit analysis = (ALE before implementing safeguard) – (ALE after implementing safeguard) – (annual cost of safeguard) [3]
== value of safeguard to the company (Urban).

As part of the safeguard cost/benefit analysis, a calculation of the Internal Rate of Return (IRR) using a Microsoft Excel spreadsheet function IRR (starting cell: ending cell, guess%) is used. Having an attractive IRR for a security improvement project proposal will definitely add momentum to your project.

5. ASSIGNING VALUES TO TANGIBLE ASSETS

The following are some typical methods for obtaining estimates for tangible assets:
(a) Ask the site controller or IT manager for cost information regarding existing equipment, software, and hardware.
(b) Conduct research on the Internet for exact or comparable systems. Determine the age of the current tangible assets, and calculate value by including depreciation.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

(c) Look for previous capital projects that contain the original cost information. Once again, make necessary adjustments based on depreciation.
(d) When determining the overall replacement cost due to total failure, be sure to include costs related to the following:
- installation cost
- troubleshooting cost
- add 10% contingency
- loss of business services to outside customers
- loss of business services to internal employees

According to the United States Bureau of Labor Statistics June 2002 Publication, fringe benefit for employees averaged 27.2% for private industry, and for government employees averaged 29.5% (US Department of Labor). Because this is a sizable amount of a typical employee's cost to a company, it should be included in the calculations for risk analysis. In other words, an employee of a private company paid $30 an hour has actually cost his company a total of $41.21/ hour (with base pay + fringe benefits).

6. ASSIGNING VALUES TO INTANGLBLE ASSETS

The typical intangible assets that are prone to information system attacks are as follows (Pavri):
- financial data
- R & D research data
- goodwill
- sales information
- marketing research
- engineering blueprints and specifications
- trade secrets and know-how
- computer software

There are two typical approaches for determining the valuation of intangible assets (Pavri):

- Cost Approach – seeks to measure an asset's fair market value, with depreciation also taken into account. This is also known as the cost of replacement. Depreciation due to physical use, functional obsolescence, and economic obsolescence must all be taken into consideration. The cost approach does not directly consider either the amount of economic benefits that can be achieved or the time period over which they might continue. A cost approach is typically used for valuing trade secrets and know-how.

- Income Approach – Focuses on the income-producing capability of the intellectual property. The value is measured by the present value of the net

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

economic benefit over the life of the asset. When the economic conditions are not favorable, the income approach leads to a relative low valuation of assets. This approach is best suited for the valuations of patents, trademarks, computer software, and copyrights.

- Relief From Royalty method: (can be used for valuing patents and trademarks) The use of an appropriate royalty rate based on information from a royalty rate database.

Always use both approaches mentioned above. Use the first one as the primary method, and the then the second one as a "sanity" check (Pavri).

Below shows a survey of how intellectual properties are typically valued in the industry.
Table 1. Valuation of Intellectual Property Survey Results (ASIS).

Valuation of Intellectual Property	Rank Order Results*							
		Industry Groups				Fiscal Year Revenues		
	All Mail Survey Responding Companies	Services	Manufacturing	High Technology	Financial	$5 BL or Less	$6 BL–$15 BL	Over $15 BL
Timing of Assignment of Value for Intellectual Property								
• Result of Litigation	1	1	3	2	2	2	1	1
• Due to Transaction	2	3	2	3	1	3	2	2
• During Licensing Negotiations	3	3	4	1	4	4	3	4
• Upon Development/Creation	4	2	1	4	3	1	4	3
• Other	5	4	5	5	5	5	5	5
Persons Responsible for Valuing IP								
• In-house Patent Council/ Legal Department	1	1	1	1	1	1	1	1
• Business Department Using IP	2	3	2	2	3	2	3	2
• CFO	3	2	3	5	2	3	2	3
• CEO	4	4	4	4	4	4	4	6
• Outside Experts	5	6	5	3	6	5	5	4
• Other	6	5	6	6	5	6	6	5
Factors Considered When Valuing IP								
• Competitive Advantage	1	1	1	1	1	1	1	1
• Incremental Profitability of IP	2	2	3	5	3	2	4	2
• R&D Costs	3	3	2	4	6	3	2	4
• Royalties to be Earned From Licensing	4	4	4	2	7	4	3	5
• Age of IP	5	5	5	6	2	6	6	3
• Other License Agreements	6	6	6	3	5	5	5	6
• Design Ability	7	8	7	8	8	8	7	7
• Convoyed Sales	8	7	8	9	4	7	8	8
• Other	9	9	9	7	9	9	9	9
Factors Considered When Valuing Damages Associated with IP								
• Loss of Competitive Advantage	1	1	2	3	2	1	2	2
• Lost Sales	2	2	3	1	1	2	1	3
• Loss of Market Share	3	3	1	2	5	3	3	1
• Lost Goodwill	4	4	5	5	3	4	5	5
• Price Erosion	5	5	4	4	6	5	4	4
• Opportunity to Secure New IP	6	6	6	6	4	6	6	6
• Other	7	7	7	7	7	7	7	7

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Valuation of intellectual property is often considered as an art rather than a science because of the very nature of the asset itself (Pavri).

An intellectual Property Example (Pavri):

Fig. 1

The Intellectual Property of Gillette:

Based on a market price of US$49 per share, Gillette had a total value of invested capital of about US$58.53 billion comprising US$54.44 billion of equity and US$4.09 billion of debt and long-term obligations (both equity and debt valued at market). The Company's various asset categories which must equal the value of total invested capital are shown below:

Gillette Company Asset Values (US$ millions)		
	Value	Total
Working Capital	$ 2,850	4.9%
Fixed/other assets	5,131	8.8%
Intangible assets	5,854	10.0%
Intellectual property	44,700	76.3%
Total invested capital	$58,535	100.0%

Notice that in the above example, the intellectual property alone for the Gillette Company is worth a whopping 76.3% of the total invested capital (Pavri). Thus, we should not underestimate the amount of damage that a computer security breach can bestow on a company's intellectual property.

7. ESTIMATING POTENTIAL THREAT AND RISK

After a vulnerability assessment and threat analysis (the discussion of threat analysis and vulnerability assessment is beyond the scope of this paper, please consult other references for details) is conducted, you can proceed to quantify the risk elements.

Please note that you do not need to calculate EF, SLE, and ARO individually if you don't have to. It would be much simpler if you can estimate ALE directly from using the data in Section 9. In addition, you will need to add a ranking number from 1 to 10 for quantifying severity (with 10 being the most severe, and 1 of least severity) as a correction factor for the risk estimate obtained from the data table in Section 9. This step is necessary because the data contained in Section 9 are general data that do not take into account of the individual risk severity differences at each company.

You can use the slide rule below in Fig. 2 to determine the matching adjustment factor with respect to the severity ranking previously chosen. The reason for this step is to

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

convert the severity ranking number to a usable number in the equation below for calculating ALE:

$ALE_{corrected} = ALE_{table} \times$ Adjustment Factor x Size Correction [4]

Fig. 2

Severity Ranking									
10	9	8	7	6	5	4	3	2	1
1.2	1.2	1.1	1.1	1.0	1.0	0.9	0.9	0.8	0.8
Adjustment Factor									

Size Correction is defined as follows:

By taking into account of the number of employees and/or annual revenue of a specific company compared to the averages as shown in Fig. 3 and/or Fig. 4, one can estimate the Size Correction:

Fig. 3

CSI / FBI 2002 Computer Crime & Security Survey

Percent		No. of Employees		
24	x	12000	=	2880
12	x	7500	=	900
27	x	3000	=	810
7	x	750	=	52.5
14	x	300	=	42
16	x	50	=	8
				4692.5

survey average 4700 employees / company

Fig. 4

ASIS Trends In Proprietary Information Loss Survey

Percent		Revenue, $BL		
57	x	3	=	1.7
23	x	10.5	=	2.4
14	x	15	=	2.1
survey average company revenue				6.2

Size Correction (for use with data obtained from Computer Security Institute)
= number of employees of the specified company / 4700

Size Correction (for use with for data obtained from ASIS)
= annual revenue of specified company / $ 6.2 billion

Example:

A company is conducting a risk analysis on laptop theft.
If it has a severity ranking of 8, the corresponding adjustment factor used will be 1.1 as shown below using Fig. 2.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Severity Ranking									
10	9	8	7	6	5	4	3	2	1
1.2	1.2	1.1	1.1	1.0	1.0	0.9	0.9	0.8	0.8
Adjustment Factor									

According to the data table in Section 9,
Company A annual revenue = $ 0.2 Billion
number of employees = 240
Size Correction (using data from CSI) = 240 / 4700 = 0.051
ALE_{table} = $ 89,000
$ALE_{corrected}$ = $ 89,000 x 1.1 x 0.051 = $ 5,000

8. ESTIMATING THE POTENTIAL EXPOSURE FACTOR

Here is a method for estimating the exposure factor for use in conducting risk analysis (feel free to modify any of the numbers below to suit your own needs and preferences):

Start off with 100% for the starting exposure factor
and answer each of the following questions ...
1. Does the system under attack have any redundancies/ backups/ copies ?
Subtract 30% if the answer is YES
2. Is the system under attack behind a firewall?
Subtract 10% if the answer is YES
3. Is the attack from outside ?
Subtract 20% if the answer is YES
4. What is the potential rate of attack? (10% damage / hour vs. 10% damage / min)
Subtract 20% if the answer is less than 20% damage/hr
Subtract 40% if the answer is less than 2% damage/hr
5. What is the likelihood that the attack will go undetected in time for a full recovery?
Subtract 10% if the probability of being undetected is less than 20%
Subtract 30% if the probability of being undetected is less than 10%
6. How soon can a countermeasure be implemented in time if at all?
Subtract 30% if the countermeasure can be implemented within ½ hour
Subtract 20% if the countermeasure can be implemented within 1 hour
Subtract 10% if the countermeasure can be implemented within 2 hours

Use the final exposure factor derived above in the equation in Section 4B for calculating ALE.

9. RISK ANALYSIS DATA

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

A. Main Data Table

Table 2 is compiled from the latest industry-wide surveys and studies. It contains many different aspects of the security risk framework. By using this table, you can take the guesswork out of estimating of the ARO, SLE, and/or ALE values for some common risk factors.

To use this table, first of all, check off at the specific risk factors that match the ones for your risk analysis. Secondly, you can identify the associated risk ARO and the losses data. The "risks ARO" column in the table contains the ARO in percentage format instead. In other words, 12% in the "risks ARO" column is equivalent to 0.12 for ARO. The "Loss Description" column contains the ALE or SLE data depending on the situation.

In addition, the word "reported" in the "Loss Description" column indicates that the quantity shown is the annual amount that is actually reported to the authorities; therefore, there is an implication that the actual security breach should be much more than the "reported" value listed in this column, since many security breaches have gone undetected and/or unreported. As a result, you may want to consider adding an additional "correction factor" when using some of the data presented in this table below to estimate ALE.

The ALE% shown in the "Loss Description" column is defined as follows:

ALE% = ALE / Asset Value [5]

Table 2. Main Data Table

Risk Factor Category	Reference Source	Threat/ Risk Description	Risks ARO	Loss Description
email	Kabay	nonproductive emails		$4,000/worker** 115hrs /worker
financial	Vijayan	credit card fraud		$580/account: SLE $7M/company
financial	Neumei-ster	credit application info.		$90/account: SLE $2.7M/company
financial	CSI	financial fraud		ALE% : 6%
financial	CSI	financial fraud	12%	$4,632,000**
information	CSI	transaction info. theft		ALE% :12%
internet	Symantec	web browser privacy	51%	
internet	CSI	insiders abuse of access	78%	$ 536,000**
internet	CSI	Denial of Service (DoS)	40%	$ 297,000**
internet	Stephens	Denial of Service (DoS) Amazon.com		200,000/hr to 300,000/hr : SLE
laptop	CSI	theft of laptop	55%	$ 89,000**
laptop	Absolute Protect	theft of laptop		1 in 14 chance per life span of laptop

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

network	CSI	sabotage of data	8%	$ 541,000**
network	CSI	active wiretapping	1%	$ 0**
network	Kensington	gross revenue		ALE%: 5.57%
network	Symantec	NetBIOS availability	20%	
overall	Symantec	virus protection ***	28%	
overall	Symantec	trojan protection ***	7%	
overall	Kabay	outside attacks	67%	
overall	Kabay	outside attacks reported		<1% reported
overall	Kabay	attacks detected		4% reported
overall	Kabay	attacks detected (rule of thumb)		approx. 10%
overall	Kabay	attacks reported to authorities (rule of thumb)		<10%
overall	CSI	security breaches	90%	
overall	CSI	attacks reported to authorities		34% reported
overall	CSI	attacks not reported		56%
overall	CSI	not report/total incidents		62%
overall	CSI	survey had companies @ $100M/yr and higher		61%
overall	CSI	system penetration	40%	$ 226,000**
overall	CSI	security breach losses	42%	$ 2M /company**
overall	Kensington	unprotected data	60%	
overall	Pescatore	insider attack on system	70%	
overall	pwcglobal.com	benchmark of IT budget dedicated to security		3 - 5% of IT budget
overall	CSI	virus attacks	85%	$ 283,000**
proprietary info.	PC Guardian	trade secret for USA		$2B /month
proprietary info.	Kabay	piracy of software sold on online auction	49%	
proprietary info.	CSI	theft of proprietary data	20%	$6,571,000**
proprietary info.	ASIS	theft of proprietary data	40%	
system	CSI	unauthorized insider access	38%	$ 300,000**
telecom	CSI	telecom fraud	9%	$ 22,000**
telecom	CSI	eavesdropping	6%	$1,205,000**

Note:

* M = million, B = billion

** These data are the ALE value

*** This is done on systems that already have anti-virus software

The above table is meant to be a living table that grows.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

B. Proprietary Information Data

For statistics specifically in regard to proprietary information losses, ASIS Survey Report 2002 is a good source of information. You will need to use Table 2.1 in the above report and Size Correction as mentioned in Section 7 to calculate the appropriate ALE (ASIS). The ASIS survey report contains data for both the average dollar value and percent of dollar loss and reported incidents of proprietary information loss listed by areas of risk (ASIS). SLE and ARO values directly related to proprietary information losses can be extracted using the above survey report.

Here is a table that shows distinct differences in companies' attitudes and "best practices" for information system security based on their propensity for loss incident reporting (ASIS). Section 4(c) describes how this table can be used.
Table 3. Opinion Survey Results (ASIS).

Attitudes and "Best Practices"	Percent[1]	
	Companies Reporting Loss Incidents	Companies Not Reporting Loss Incidents
Information associated with new products and services is vital to the success of our company	75	73
The Internet, networks, and computers and related technologies have created significant new threats to sensitive proprietary information	75	59
Only people with a need to know are given access to sensitive information	40	75
Information security is a priority within our company	45	71
Physical security in my location is adequate to safeguard sensitive documents	44	71
We require everyone to use screen savers and/or server passwords to protect computer systems when unattended	47	66
Our company's policies/guidelines concerning safeguarding sensitive/proprietary information are fit for the purposes for which they were intended	42	69
Non-disclosure agreements are effectively used in our company	49	60
Management is concerned about information loss and takes necessary precautions	36	67
Sensitive information is not seriously at risk in our organization	31	66
Our company has effective information system security procedures	38	64
Our company has not discovered vulnerabilities to electronic means of information gathering ("bugging devices") during assessments of offices and meeting rooms	49	58
Our company has not discovered vulnerabilities to electronic means of information gathering ("bugging devices") during assessments of telecommunications cables and equipment	47	53

1 Percent is based on "strong agreement" ratings from 138 responding companies.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

10. METHOD OF DATA INTERPRETATION

The survey information in Table 4 can be used for the adjustment of the relative importance of risk factors contained in a quantitative risk analysis based on the type and size of the company. This is important because even if a risk factor is deemed financially attractive to pursue, it may turn out that the particular risk factor in question is not perceived as being important by the particular industry sector and company size (as we may find out by using Table 4.) In cases where there is a tie between two risk factors, the information below can be used to break the tie by having to select the one that is perceived as being more important.

Table 4. Attitudes and "Best Practice" Strategies vs. Classification Categories (ASIS).

Strongly Held Attitudes and "Best Practice" Strategies	All Responding Companies	Industry Group				Fiscal Year Revenues			Companies Reporting Loss Incidents	Companies Not Reporting Loss Incidents
		Services	Manufacturing	High Technology	Financial	$5 BL or Less	$5 BL–$15 BL	Over $15 BL		
Information associated with new products and services is vital to the success of our company	1	1	1	1	1	1	1	2	1	2
The Internet, networks, and computers and related technologies have created significant new threats to sensitive proprietary information	2	4	2	2	*11	9	2	1	2	11
Only people with a need to know are given access to sensitive information	3	3	7	3	5	2	8	7	*10	1
Information security is a priority within our company	4	7	4	4	4	4	5	4	*7	3
Physical security in my location is adequate to safeguard sensitive documents	5	8	6	7	2	5	9	3	*8	4
We require everyone to use screen savers and/or server passwords to protect computer systems when unattended	6	11	7	6	3	3	6	13	*5	7
Our company's policies/guidelines concerning safeguarding sensitive/ proprietary information are fit for the purposes for which they were intended	7	2	11	8	6	7	4	5	*9	5
Non-disclosure agreements are effectively used in our company	8	*13	3	5	*13	11	3	8	*3	10
Management is concerned about information loss and takes necessary precautions	9	9	8	9	*12	10	7	9	*12	6

In using your own sets of data or information obtained from industry research for security risk analysis, you can use the data from the US Census below to calculate the Size Correction (as discussed in Section 7.) Use the data from the Excel table from the

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

U.S. Census to calculate the Size Correction (US Census). You can also Table 2a & 3 from the U.S. Census if you cannot identify the proper category for your company as described in Excel table (US Census).

11. OVERSEAS RISKS AND THREATS

Apart from the computer security issues and reports in the United States, 66% of British firms have suffered a serious incident such as hacking, virus attacks or credit card fraud within the last year during a recent survey (Kensington). For the first time ever, most of the incidents originated from outside of the company, not inside of the company. In addition, negative publicity rather than direct financial loss harmed their businesses the most (Kensington). Meanwhile in another survey, it is reported that 44% of British firms have suffered at least one malicious security breach in the past year, which is nearly double the numbers in the 2000 survey. The average cost of a serious security incident in UK is 30,000 British pound (pwcglobal). Virus infection is the number one most serious security breach in UK; it is recorded at 33% (PricewaterhouseCoopers).

British companies consist mostly of small businesses; 97.6% of all British companies are small businesses with less than 50 employees. Only 0.5% have more than 250 employees. As a result of their smaller sizes, their information systems security stance will be different from ours (PricewaterhouseCoopers).

A Survey has discovered that only 15% of British IT security personnel knew the contents of BS7799 (the British Standard for Information Security Management) In addition, only 51% of UK transactional websites currently use encryption to protect their customers' security. Only 19% of businesses currently use the more secure public key encryption. Furthermore, only 27% of UK firms have security policies in place (PricewaterhouseCoopers). Indeed, one can clearly see that the potential for fraud and subsequent damage is enormous.

12. LAPTOP SECURITY

The average financial loss of a stolen laptop is $89,000. Only a small percentage of the $89,000 is the actual hardware (Computer Security Institute). A handy tool offered by Kensingtion, a company that makes laptop security cable systems, can help you to calculate the ROI for laptop hardware physical security protection. You can readily modify this tool to fit your individual needs (Kensington). In 2000, almost 390,000 notebook computers were stolen in the USA. But in 2001, about 591,000 laptops were stolen - an increase of more than 50%. That works out to more than 1,600 notebook computers stolen every day (PC Guardian). In addition, the FBI estimates that 57% of unauthorized intrusions into corporate servers are made possible through the use of stolen notebooks, which provide remote access capability, passwords, information about the location of sensitive or confidential information, and employee contact information (PC Guardian). Today hackers even have a "bounty" out for notebooks

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

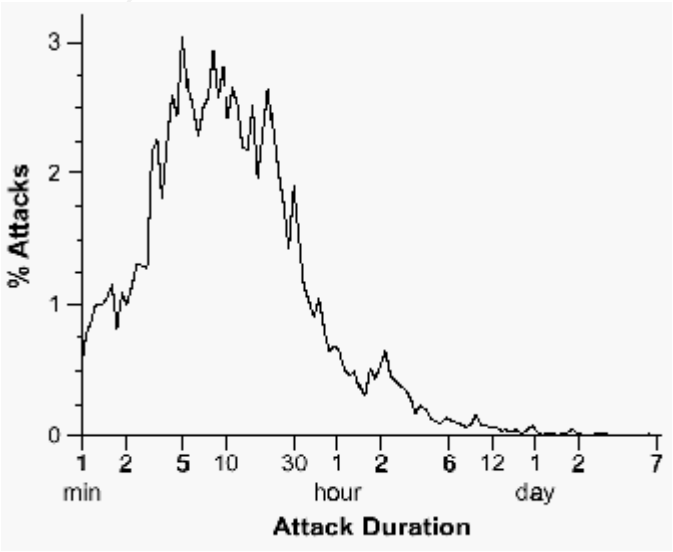
stolen from key executives of certain companies and government agencies (PC Guardian). Insurance statistics show that if you own a laptop you have a 1 in 14 chance that it will be stolen (Absolute Protect).

13. INTERNET THREATS / ISSUES

For the fifth year in a row, more respondents in the CSI/FBI 2002 survey (74%) cited their Internet connection as a frequent point of attack than their internal systems (33%) (Computer Security Institute). 78% percent detected employee abuse of Internet access privileges (for example, downloading of pornography or pirated software, or inappropriate use of e-mail systems) (Computer Security Institute). If these behaviors remained unchecked, this could lead to potentially serious sexual harassment lawsuits by coworkers.

38 percent suffered unauthorized access or misuse on their websites within the last twelve months. 21 percent said that they didn't know if there had been unauthorized access or misuse. 40 percent also detected denial of service attacks. (Computer Security Institute). Until recently there had not been any documented study of the overall severity of global DoS in the World Wide Web. However, by using a new technique called a "backscatter analysis", David Moore and his colleagues from the University of California at San Diego had set out to determine the total number of worldwide DoS (denial of service attacks). They studied the entire World Wide Web over a period of 3 weeks during February 2002. 12,805 attacks on 5000 distinct targets in more than 2000 distinct DNS domains were found as a result of the study. The targets included big names such as Amazon and Hotmail. One important finding from the research is that it is estimated that 46% of all attack events have rates of 500 packets per second or higher, which can easily overwhelm servers that are without specifically-configured firewalls. The hosts that were attacked ranged from ARPA, broadband, dial-up, IRC server, nameserver, router, web server, firewall, and many others (Moore). Fig. 5 shows the distribution of durations of DoS attacks in his study.

Fig. 5 World-Wide DoS Attack Duration Distributions (Moore).



© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The CSI/FBI 2002 Computer Crime & Security Survey contains several charts useful for calculating the ARO for internet related attacks (Computer Security Institute).

14. CONCLUSIONS

In this paper, the following components for a quantified risk analysis are discussed:

- Reasons for doing a quantitative analysis instead of a qualitative version
- A centralized table of data and facts for calculating ARO and ALE
- Methods to characterize difficult assets such as intellectual property and proprietary information
- A process plan for conducting quantitative risk analysis
- New techniques and adaptations in aiding to calculate some of the needed key variables

One important aspect to consider is that a security countermeasure may have to be implemented anyway regardless of whether or not it had been turned down the first time around. This is simply because that an unfortunate security breach may have occurred because of the decision made to forego with the countermeasure during the first time around. Therefore, it becomes merely a question of “pay now, or pay later”. Another fact to think about is that money spent on security improvements is similar to that for insurance premiums to guard against unexpected catastrophic losses. Therefore, security costs are similar to insurance expenses. They are both part of the costs of doing business.

Apart from the currently known risks, and their associated costs, companies that do not have consistent and verifiably appropriate security practices for protecting their IT assets are opening themselves up to liability lawsuits, warned by security expert. "You can expect to see major liability lawsuits in the next 18 months" or so, said Randy Marchany, a member of the Virginia Tech Computing Center's systems management group and the coordinator of its Computer Incident Response Team, speaking at the SANS 2001 technical conference in Baltimore. Increasingly, companies that fail to show due diligence in minimizing their exposure to such threats will become targets for lawsuits, agreed Margaret Jane Radin, a professor of law, science and technology at Stanford University Law School. Legal liability in such cases is likely to depend on what prevention technologies and practices are available and on whether these technologies and practices are reasonably cost-effective to implement, she said (Vijayan).

As a result, showing due diligence will mean everything from implementing technologies such as firewalls, intrusion-detection tools, content filters, traffic analyzers and virtual private networks to having best practices for continuous risk assessment and vulnerability testing. It will also mean having corporate policies and procedures backing up all of this, as analysts have said (Vijayan). As one can see, the arena of cost justification of security countermeasures in the war against computer crime will likely

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

become much larger in the future. Besides the current justifications for protecting against stolen information, laptop theft, financial fraud, etc., we may be looking at the financial implications of multi-million dollar class-action lawsuits in the years to come. Therefore, a future paper on quantitative risk analysis may have to devote a chapter to tort law.

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

References:

Absolute Protect. "Computer Theft Statistics." URL: http://www.absolute-protect.com/statist.htm (10 December 2002).

ASIS International. "Trends In Proprietary Information Loss Survey Report." September 2002. URL: http://www.asisonline.org/pdf/spi2.pdf (10 December 2002).

Computer Security Institute (CSI) . "2002 CSI/ FBI Computer Crime and Security Survey." Computer Security Issues & Trends. Vol. 8, No. 1 Spring 2002. URL: http://www.gocsi.com/pdfs/fbi/FBI2002.pdf (10 December 2002).

Consumer.gov "Cases & Scams." 7 August 2002. URL: http://www.consumer.gov/idtheft/cases.htm (10 December 2002).

Kabay, M. E.. "Studies & Surveys of Computer Crime." Computer Security Handbook, 4th Ed. January 2001. URL: http://www.cybersecure.ca/sscc.pdf (10 December 2002).

Kensington Technology Group. "ROI Calculator." URL: http://www.microsaver.com/index.html (10 December 2002).

Miller, Jean. "Risk Management for Your Web Site." International Risk Management Institute Expert Commentary. September 2000. URL: http://www.irmi.com/expert/articles/schoenfeld003.asp (10 December 2002).

Moore, David et. al. "Inferring Internet Denial-of-Service Activity." Cooperative Association for Internet Data Analysis, San Diego Supercomputer Center, University of California, San Diego. 2001. URL: http://www.caida.org/outreach/papers/2001/BackScatter/index.xml (10 December 2002).

Neumeister, Larry. "U.S. Charges 3 in ID Theft of 30,000. " Associated Press. 26 November 2002. URL: http://story.news.yahoo.com/news?tmpl=story&u=/ap/20021126/ap_on_re_us/identity_theft_13 (10 December 2002).

Pavri, Zareer. "Valuation of Intellectual Property Assets: The Foundation for Risk Management and Financing." PricewaterhouseCoopers. 29 April, 1999. URL: http://www.pwcglobal.com/extweb/manissue.nsf/DocID/1628AF8B3C99F360852567BB006D8B24 (10 December 2002).

PC Guardian. "Computer Crime Stats." URL: http://www.pcguardian.com/portal/crimestats.html (10 December 2002).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Pescatore, John. "High-Profile Thefts Show Insiders Do the Most Damage." Gartner, Inc. In The News. 26 November 2002. URL: http://www4.gartner.com/DisplayDocument?doc_cd=111710 (10 December 2002).

PricewaterhouseCoopers. "Information Security Breaches Survey 2002 Technical Report." 23 April 2002. URL http://www.pwcglobal.com/Extweb/ncsurvres.nsf/docid/845A49566045759E80256B9D003A4773 (10 December 2002).

pwcglobal.com "Information Security Breaches Survey 2002." PricewaterhouseCoopers Executive Summary. April 2002. URL: http://www.pwcglobal.com/Extweb/ncsurvres.nsf/0cc1191c627d157d8525650600609c03/845a49566045759e80256b9d003a4773/$FILE/ExecSumm_Final_220302.pdf (10 December 2002).

Stephens, Justin. "The Changing Face of Distributed Denial of Service Mitigation." SANS Institute Information Security Reading Room. 16 August 2001. URL: http://rr.sans.org/threats/face.php (10 December 2002).

Symantec Corporation. "Security Risk Statistics." Symantec Security Check. URL: http://security1.norton.com/ssc/sc_stats.asp?j=1&langid=ie&venid=sym&plfid=20&pkj=TFDVWHFHMFNZMBBXLKU (5 December 2002).

Urban, Carol. "Security Risk Management." Azsage Presentation. 11 September 2002. URL: http://www.azsage.org/present/091102/RiskMgmt.ppt (10 December 2002).

U.S. Census Bureau. "Statistics of US Businesses." 1999. URL: http://www.census.gov/csd/susb/usalli99.xls (10 December 2002).

U.S. Department of Labor Bureau of Labor Statistics News. "Employer Cost for Employee Compensation – June 2002." 17 September 2002. URL: ftp://ftp.bls.gov/pub/special.requests/ocwc/ect/ececrlse.pdf (10 December 2002).

Vijayan, Jaikumar. "IT security destined for the courtroom." Computerworld, Inc.. May 21, 2001. URL: http://www.computerworld.com/governmenttopics/government/legalissues/story/0,10801,60729,00.html (10 December 2002).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 24th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced