A Method for Quantitative Risk Analysis

By James W. Meritt, CISSP

I Introduction

There are two primary methods of risk analysis and one hybrid method:

- ***Qualitative*** - Improve awareness of Information Systems security problems and the posture of the system being analyzed.
- ***Quantitative*** - Identification of where security controls should be implemented and the cost envelope within which they should be implemented.
- ***Hybrid method*** - A selected combination of these two methods can be used to implement the components utilizing available information while minimizing the metrics to be collected and calculated. It is less numerically intensive (and less expensive) than an in-depth exhaustive analysis.

The first, qualitative analysis, is simpler and widely used. Qualitative analysis helps in the identification of the assets and resources at risk, vulnerabilities that might allow the threats to be realized, safeguards already in place and those which may be implemented to achieve an acceptable level of risk and increase overall awareness. This analysis uses simple calculations and uses procedure in which it is not necessary to determine the dollar value of all assets and the threat frequencies or the implementation costs of the controls. Quantitative analysis does this as well as identifies the specific envelope in which the losses and safeguards exist. It is based substantially on independently objective processes and metrics and requires an accordingly increased degree of effort be placed in deterring the cost values and an increasing amount of effort be placed into the calculations. It does, however, present its results in a management-friendly form of monetary values, percentages, and probabilities. Since the Office of Management and Budget Circular A-130 no longer requires a full-blown risk analysis the hybrid model using a facilitated risk analysis process is gaining in popularity due to its reduced costs and efforts required in spite of not providing the metrics desired for management decisions.

II Methodology

1. Scope Statement

The scope statement is your first step. This single statement is what you will give to the Information Technology Committee meeting recorder, incorporate into the submitted proposal. The scope statement must be committed to by all concerned.

The scope statement must:

a. Specify exactly what is to be evaluated
b. State what kind of risk analysis will be performed
c. Provide the expected results

For example "A quantitative risk analysis will be performed on the Glimby information system to determine what controls, if any, are needed to reduce the risks to the system to an acceptable level using benefit-cost analysis methodologies for determining applicable controls."

2. Asset pricing

The information system specified in the scope statement next will be broken down into its components which will then be individually priced. While it is possible to break down the system into functional units, I find it much easier to disassemble the overall system into its tangible components which may be more easily priced. I recommend the following breakdown:

Network/telecommunications: Modems - This category consists of the various modems both internal and external. Any system used to connect information systems to communication lines is contained within this category

Network/telecommunications: routers - This category contains those items of information technology which are identified as routers, gateways, hubs or serve a similar purpose.

Network/telecommunications: Cabling - This category includes special purpose cabling identified for the information technology but does not include that which is installed as part of the operating area (e.g. built in).

Network/telecommunications: Other - This category includes those items of information technology that are used for networking and/or telecommunications but do not fit within other designated categories. It includes, but is not limited to, special-purpose communication cards and adapters.

Software: Operating System - This is the programming, which enables the information technology to operate. The vendor along with the hardware that it operates provides it. Examples are MVS, DOC, UNIX, …

Software:Applications - This category contains those items of software which are directly necessary for the business operations of the organization. It is usually developed in-house or under contract and does not contain those items of software directly necessary for the operations of systems within it.

Software: Other - This includes any programming which is not either identified as a component of a system Operating System or as one of the primary applications. Typical examples are provided by third-party vendors.

Equipment: Monitors - This category covers items which are used to display information from the various units of information technology. It contains, but is not limited to, stand-alone computer monitors and terminals.

Equipment: Computers - This category includes all information processing equipment maintained by the organization. It contains, but is not limited to, PCs, front-end processors, fileservers, mainframe computers and workstations.

Equipment: Printers - This category contains items of information technology used to impress information upon paper. It includes things such as a variety of printers (varying from dot matrix through laserprinters) and plotters.

Equipment: Other - This category contains items of equipment not covered by other designated categories. It contains, but obviously is not limited to, such things as memory cards, disk drives, tape units and power supplies.

Data/information: System - This category includes that information which is maintained for the operation of the information system. It includes, but is not limited to, such things as schedule information, error logs, usage logs, and similar logging data.

Data/Information: Business - This category includes that information maintained for the business purposes of the overall organization. The system business databases, for example, would be included in this category.

Data/Information: Other - This category includes all information sources not readily identifiable as belonging in one of the other two.

Other:Facilities - This may be the entire building itself and its supplied services or simply the table the system is on. It depends, of course, on the system being analyzed.

Other: Supplies - This includes supplies for the information system. Included are such things as spare parts, backup components, repair kits, paper,… It does NOT include supplies for non-IS functions associated with the business.

Other: Documentation - This is the documentation associated with the operation of the information technology. It does NOT include that documentation which may be present for non-IS purposes.

Other: Personnel: - These are the people which work with the information system in all capabilities. It does not include manning at the organization for non-IS duties. As a first-order estimate the sum of salaries of all operating personnel may be used, as long as you remember that there are non-tangible assets such as experience and loyalty which are not necessarily appropriately priced.

It is a basic axiom that you should not spend more protecting an asset than that asset is worth. So by completing this exacting process of enumerating and pricing you components of the information system under consideration you have established a number of upper thresholds for system safeguards.

This leaves the intangible assets involved, such as client confidence and experience. These things, while important, are not so easily priced and will not be included in the quantitative analysis but it must be remembered that they are present and will be included in deciding what risks have been reduced to acceptable limits, controls and rate a special mention in the final report.

III. Risks

A *risk* to the information system is something that can, in some way, cause harm or reduce the operational utility of the system. *Threats* are those things which may occur independent of the system under consideration and which may pose the risk.

The threats considered are:

Power Loss - The loss of the electrical power supply to the information systems.

Communication Loss - The inability to transfer information to and from the organization through the defined system parameter.

Data Integrity Loss - A realized, or perceived possible, alteration of the data and/or information maintained by or consisting of the specified asset.

Accidental Errors - Improper use of information technology not due to malicious intent but solely through mistaken incorrect use

Computer Virus - A Program which spreads by attaching itself to "healthy" programs. After infection, the program may perform a variety of non-desirable functions.

Abuse of Access Privileges by Employees - Employees are authorized by the Security Policy of the organization and further narrowed by their job responsibilities to perform a small selection of functions with the information system. This category covers those acts which may be performed but which are not authorized.

Natural Disasters - Those occurrences which degrade some aspect of the information system other than fire and earthquake and are not manmade. Examples would be flooding, a tornado,…

Attempted Unauthorized System Access by Outsider - Non-employees or personnel not contracted to perform work with or on the information system who are not appropriately authorized yet are attempting, but not succeeding, in gaining access to the information system.

Theft or Destruction of Computing Resource - A primary resource of the organization is the computing capability of its information systems. This threat addresses the unauthorized use of this resource and the destruction of this resource - through physical or other means.

Destruction of Data - Information held by an organization is not only that used by their business applications, but includes that used by the systems to operate, manuals, personal experience and other forms. This threat may destroy that information, or simply prevent the organization from using it.

Abuse of Access Privileges by Other Authorized User - While an employee is authorized to perform - and indeed may be required - to perform many actions using the information system, he or she limited to what may be done through organizational policy, job restrictions and technological controls. But an authorized user - whether an employee or contractor - may attempt to perform operations which are denied them.

Successful Unauthorized System Access by Outsider - This covers non-employees and non-contractors using, and possibly destroying, information system resources. "Hackers" fit within this threat description.

Non-disaster downtime - This covers those times when the information system is unavailable for use not caused by disaster. Examples of this would be maintenance, component failure and the system 'crashing'.

Fire - This includes both major fires that destroy resources to those which prevent assets from being used for any reason.

Earthquake - This includes both directly destructive and influences of lesser and distant 'quakes.

A magazine survey in *Information Week* (October 1996) asked "What Security Problems have resulted in financial losses?" Another magazine survey, in *InfoSecurity News* May 1997 asked "In the past 12 months, which of the following breaches have you experienced?" The following statistics are the results of combining the information from these surveys. The number is the number of times that particular threat may be expected to happen in one year.

Power loss:	2.00
Communication Loss:	2.00
Data Integrity Loss:	2.00
Accidental Errors:	.72
Computer Virus:	.68
Abuse of Access Privileges by Employees:	.4
Natural disasters:	.29
Attempted Unauthorized System Access by Outsider:	.27
Theft or Destruction of Computing Resource:	.24
Destruction of Data:	.17
Abuse of Access Privileges by Other Authorized User:	.09
Successful Unauthorized System Access by Outsider:	.08
Non-disaster downtime:	.06

Fire:	.01
Earthquake:	.01

This leaves some risks for which statistical information is not available but is nonetheless important. Examples (not to be taken as exhaustive) are:

- Access via "back doors" created by application developers
- Improper editing routines for data entry functions
- Improper editing routines for external feeds
- Timeliness of external feeds
- Program bugs
- Lack of Change Control Process
- Lack of Version Control Process
- Corrupted Data base
- Can't accept Year 2000 or greater
- Unattended workstations
- Hardcopy management
- User awareness
- Servers unavailable
- Wide Area Network unavailable
- Lack of proper backups

IV. Exposure/Impact coefficient

All assets are not equally vulnerable to every risk. The degree to which an identified asset is vulnerable to a specified risk may vary from totally invulnerable (example: cabling systems are reasonably invulnerable to computer virus infections) to absolutely destroyed (example: printers. Once they are stolen, result in a total loss).

While the possibility of a particular threat of occurring doesn't change regardless of the controls implemented for the system, the degree to which the system is vulnerable to the threat may be reduced. This is the value which may be modified to compensate for already-implemented controls.

Using the threats identified is (3) above against the assets components recommended in (2), the following coefficients are recommended as initial values. Please note that they must be individually investigated and approved or modified to suit local conditions.

Expected losses are based upon the anticipated effect of threats on assets and processes. The amount of the loss depends on the vulnerability of an asset or process to a given threat. The vulnerability factor (0.0 to 1.0) of an asset with respect to a threat is the ratio of:

(1) the expected loss from a single impact of the threat on the asset to
(2) The loss potential of the asset.

Different assets respond differently to different realized threats. The effectiveness of particular threats against varying assets are different from "no impact" to "total replacement necessary" depending upon the sensitivity of the asset and threat under consideration. What follows is a first-order evaluation of this sensitivity. The threats considered are REALIZED - they are assumed to have occurred. The likelihood of a particular threat occurring is considered separately and will not be contained within this evaluation. The SLE (single loss expectancy) is given as a value between 0 and 1 and represents the damage to the asset. Sample values are:

Value	Description
0	The asset is resistant to the threat and no damage results from the realization of the threat.
.3	When the threat occurs, there is usually no damage resulting but it is possible that catastrophic damage will result requiring total replacement.
.5	When the threat occurs it is equally likely that no damage will result or that total replacement will be necessary. All outcomes between these extremes are equally likely.
.7	After a successful threat is executed, the effected system will usually require replacement. On occasion - if you are lucky - it will miss total damage, possibly even entirely.
1	When the threat is realized, total replacement of the identified asset is the only outcome possible.

See Appendix A. for sample values. These values were arrived at in consultation with numerous subject-matter experts.

V. Group Evaluation

A group evaluation meeting should next be held that is composed of the stakeholders (those with a vested interest) of the system. This meeting includes individuals who have knowledge of the various components in, threats to and vulnerabilities of the system as well as management/operations responsibilities to help in the determination of overall acceptability. This structured meeting is greatly like that advanced by the hybrid facilitated risk analysis methodology developed initially by the Computer Science Institute.

The meeting provides a common focus on the methodology among the various stakeholders and business units. It is up to you to maintain an open and balanced flow through the meeting by providing clearly defined roles and responsibilities for the various members and to identify or verify:

a. Assets
b. Risks
c. Exposure/Impact

d. Acceptability determination

The overall meeting time should be approximately 4 hours. The facilitator (you) should already have the numbers ready and waiting with just a few blanks to be filled in. If possible, disseminate the information a day or more earlier when you give out the agenda and attendee list so that the participants may research any value they question or need to provide as you rapidly go through the form.

Be careful not to get out of scope, addressing areas of concern or disagreements that are not relevant to the scope statement (see section I). For anything that may come up that is plainly important but out of scope, write it down for later consideration and move on.

Make special note of any area that is determined to already be at or near acceptable risk levels, as determined by the appropriate members. By acceptable items from the list and concentrating on those near acceptability you may narrow the focus of your post-meeting calculations.

VI. Calculation

The values were entered into a simple spreadsheet which contained the assets on one axis, the threats on the other and the vulnerability coefficient at their intersection. The second sheet contained a table with similar threat and asset values, but the intersection points were the product of the particular asset times the probability of the threat times the vulnerability of that specific asset to that specific threat.

VII. Analysis

a. Across asset - A sum of the product of terms was made across each asset for all threats. This summation gives the expected annual loss to that asset for all threats. Looking across these terms will show you which assets need the most protection (the most can be lost there).

b. Across risk - A sum of the product of terms was made across each threat for all assets. This summation gives the expected annual loss due to that threat to the entire system. Looking across these terms will show you what threats need to be guarded most against (the most can be lost to them)

The sum of all the values in (a) should be the same as the sum of all values in (b). This value is the **A**nnual **L**oss **E**xpectancy (ALE) for the entire system to all threats.

VIII. Controls

Controls are those things which are implemented to prevent the exposure to the threat in the first place, detect if the threat has been realized against the system, mitigate the impact of the threat against the system or to recover/restore the system. Examples of possible controls are:

- Develop, document, and test backup procedures
- Develop, document, and test continuity of operations procedures
- Implement and access control mechanism
- Implement user authentication mechanism
- Implement encryption mechanism
- Implement a configuration management process for software
- Implement a version control process for documentation
- Prepare, distribute, and maintain plans, instructions, guidance, and standard operating procedures concerning the security of the system operation
- Develop user documentation on proper use of the system
- Conduct training on the proper and secure use of the system
- Implement mechanisms to monitor, report and audit activities identified as requiring independent review
- Implement operations controls to ensure proper separation of data
- Negotiate maintenance or supplier agreements to facilitate the continued secure operational status of the system
- Ensure consultation with Facilities Management to implement physical security controls to protect the system
- Ensure appropriate personnel security investigations are performed
- Implement QA performance monitoring/testing procedures
- Ensure LAN Administration installs the corporate standard anti-viral software throughout the system
- Train backup personnel
- Request management support to ensure the cooperation and coordination of various business units
- Production Management controls such as search and remove processes to ensure data stores are clean
- Time requirements will be tracked for technical maintenance
- Document possible security exposures such as program access "backdoors"
- Backup sites (hot or cold sites) locations and requirements determined and appropriately implemented
- Test for Y2K compliance

Please note that this list consists of **EXAMPLES** and is not exhaustive

The controls, once the candidates have been identified or discarded by the group meeting, must be analyzed. Two recommended methods are:

a. *Cost/Benefit ratio* - Where the reduction in the ALE when applying the particular control across all assets and all threats is compared to the local cost for implementing the control. Another basic axiom is that you should not invest more in the control (cost) than it would be worth (benefit). Hence, no system which has a cost/benefit ratio of 1 or above should even be a candidate for implementation. This affords yet another upper threshold that you could not get without performing a quantitative analysis.

b. *Risks/Control* (e.g. "bang per buck") - Where the risks reduced by the control are enumerated (either by count or summed ALE reduction) are compared to the control (either unity or implementation cost). This is a method utilized in qualitative analysis that may be used or enhanced by quantitative methods.

These ratios are then compared to determine which - if any - of the controls may best be implemented.

IX. Conclusion

It is possible to answer management's questions which inevitably turn to costs and other metrics. While there are a number of intangible assets and unquantifiable risks it is possible to perform some basic mathematical calculations yielding results which may give firm guidance towards improving the security of any system.

Appendix A: Exposure/Impact coefficient

These values were derived using the combined experience and skills of a number of experts in the arena of information systems security. They are suggested values and do not take the local threat environment or existing countermeasure effectiveness into account.

Network/telecommunications: Modems

For threat:

Power loss:	0.20
Communication Loss:	0.40
Data Integrity Loss:	0.00
Accidental Errors:	0.10
Computer Virus:	0.30
Abuse of Access Privileges by Employees:	0.10
Natural disasters:	0.50
Attempted Unauthorized System Access by Outsider:	0.20
Theft or Destruction of Computing Resource:	1.00
Destruction of Data:	0.00
Abuse of Access Privileges by Other Authorized User:	0.00
Successful Unauthorized System Access by Outsider:	0.10
Non-disaster downtime:	0.20
Fire:	0.30
Earthquake:	0.30

Network/telecommunications: Routers

For threat:

Power loss:	0.40
Communication Loss:	0.50
Data Integrity Loss:	0.10
Accidental Errors:	0.10
Computer Virus:	0.10
Abuse of Access Privileges by Employees:	0.20
Natural disasters:	0.50
Attempted Unauthorized System Access by Outsider:	0.10
Theft or Destruction of Computing Resource:	1.00
Destruction of Data:	0.10
Abuse of Access Privileges by Other Authorized User:	0.00
Successful Unauthorized System Access by Outsider:	0.20
Non-disaster downtime:	0.10
Fire:	0.30

Earthquake:	0.30

Network/telecommunications: Cabling

For threat:

Power loss:	0.10
Communication Loss	0.10
Data Integrity Loss:	0.00
Accidental Errors:	0.30
Computer Virus:	0.00
Abuse of Access Privileges by Employees:	0.50
Natural disasters:	0.50
Attempted Unauthorized System Access by Outsider:	0.50
Theft or Destruction of Computing Resource:	1.00
Destruction of Data:	0.00
Abuse of Access Privileges by Other Authorized User:	0.00
Successful Unauthorized System Access by Outsider:	0.50
Non-disaster downtime:	0.10
Fire:	0.30
Earthquake:	0.30

Network/telecommunications: Other

For threat:

Power loss:	0.20
Communication Loss:	0.10
Data Integrity Loss:	0.00
Accidental Errors:	0.20
Computer Virus:	0.00
Abuse of Access Privileges by Employees:	0.30
Natural disasters:	0.50
Attempted Unauthorized System Access by Outsider:	0.00
Theft or Destruction of Computing Resource:	1.00
Destruction of Data:	0.00
Abuse of Access Privileges by Other Authorized User:	0.00
Successful Unauthorized System Access by Outsider:	0.20
Non-disaster downtime:	0.10
Fire:	0.30
Earthquake:	0.30

Software: Operating System

For threat:

Power loss:	0.20
Communication Loss:	0.10
Data Integrity Loss:	0.00
Accidental Errors:	0.10
Computer Virus:	0.80
Abuse of Access Privileges by Employees:	0.20
Natural disasters:	0.50
Attempted Unauthorized System Access by Outsider:	1.00
Theft or Destruction of Computing Resource:	1.00
Destruction of Data:	0.00
Abuse of Access Privileges by Other Authorized User:	0.00
Successful Unauthorized System Access by Outsider:	0.60
Non-disaster downtime:	0.05
Fire:	0.30
Earthquake:	0.30

Software:Applications

For threat:

Power loss:	0.10
Communication Loss:	0.10
Data Integrity Loss:	0.00
Accidental Errors:	0.40
Computer Virus:	0.30
Abuse of Access Privileges by Employees:	0.20
Natural disasters:	0.50
Attempted Unauthorized System Access by Outsider:	0.30
Theft or Destruction of Computing Resource:	1.00
Destruction of Data:	0.00
Abuse of Access Privileges by Other Authorized User:	0.00
Successful Unauthorized System Access by Outsider:	0.60
Non-disaster downtime:	0.20
Fire:	0.30
Earthquake:	0.30

Software: Other

For threat:

Power loss:	0.10
Communication Loss:	0.10
Data Integrity Loss:	0.00
Accidental Errors:	0.10
Computer Virus:	0.20
Abuse of Access Privileges by Employees:	0.20

Natural disasters:	0.50
Attempted Unauthorized System Access by Outsider:	1.00
Theft or Destruction of Computing Resource:	1.00
Destruction of Data:	0.00
Abuse of Access Privileges by Other Authorized User:	0.00
Successful Unauthorized System Access by Outsider:	0.20
Non-disaster downtime:	0.20
Fire:	0.30
Earthquake:	0.30

Equipment: Monitors

For threat:

Power loss:	0.00
Communication Loss:	0.00
Data Integrity Loss:	0.00
Accidental Errors:	0.10
Computer Virus:	0.00
Abuse of Access Privileges by Employees:	0.00
Natural disasters:	0.50
Attempted Unauthorized System Access by Outsider:	0.00
Theft or Destruction of Computing Resource:	1.00
Destruction of Data:	0.00
Abuse of Access Privileges by Other Authorized User:	0.00
Successful Unauthorized System Access by Outsider:	0.10
Non-disaster downtime:	0.00
Fire:	0.30
Earthquake:	0.30

Equipment: Computers

For threat:

Power loss:	0.20
Communication Loss:	0.20
Data Integrity Loss:	0.00
Accidental Errors:	0.70
Computer Virus:	0.50
Abuse of Access Privileges by Employees:	0.40
Natural disasters:	0.50
Attempted Unauthorized System Access by Outsider:	0.20
Theft or Destruction of Computing Resource:	1.00
Destruction of Data:	0.00
Abuse of Access Privileges by Other Authorized User:	0.00
Successful Unauthorized System Access by Outsider:	0.80

Non-disaster downtime:	0.20
Fire:	0.30
Earthquake:	0.30

Equipment: Printers

For threat:

Power loss:	0.10
Communication Loss:	0.10
Data Integrity Loss:	0.00
Accidental Errors:	0.10
Computer Virus:	0.05
Abuse of Access Privileges by Employees:	0.10
Natural disasters:	0.50
Attempted Unauthorized System Access by Outsider:	0.10
Theft or Destruction of Computing Resource:	1.00
Destruction of Data:	0.00
Abuse of Access Privileges by Other Authorized User:	0.00
Successful Unauthorized System Access by Outsider:	0.15
Non-disaster downtime:	0.05
Fire:	0.30
Earthquake:	0.30

Equipment: Other

For threat:

Power loss:	0.20
Communication Loss:	0.10
Data Integrity Loss:	0.00
Accidental Errors:	0.20
Computer Virus:	0.30
Abuse of Access Privileges by Employees:	0.10
Natural disasters:	0.50
Attempted Unauthorized System Access by Outsider:	0.10
Theft or Destruction of Computing Resource:	1.00
Destruction of Data:	0.00
Abuse of Access Privileges by Other Authorized User:	0.00
Successful Unauthorized System Access by Outsider:	0.30
Non-disaster downtime:	0.20
Fire:	0.30
Earthquake:	0.30

Data/information: System

For threat:

Power loss:	0.20
Communication Loss:	0.06
Data Integrity Loss:	0.97
Accidental Errors:	0.50
Computer Virus:	0.95
Abuse of Access Privileges by Employees:	0.30
Natural disasters:	0.50
Attempted Unauthorized System Access by Outsider:	1.00
Theft or Destruction of Computing Resource:	0.02
Destruction of Data:	1.00
Abuse of Access Privileges by Other Authorized User:	0.30
Successful Unauthorized System Access by Outsider:	0.70
Non-disaster downtime:	0.20
Fire:	0.30
Earthquake:	0.30

Data/Information: Business

For threat:

Power loss:	0.10
Communication Loss:	0.30
Data Integrity Loss:	0.70
Accidental Errors:	0.50
Computer Virus:	0.30
Abuse of Access Privileges by Employees:	0.50
Natural disasters:	0.50
Attempted Unauthorized System Access by Outsider:	0.30
Theft or Destruction of Computing Resource:	0.40
Destruction of Data:	1.00
Abuse of Access Privileges by Other Authorized User:	0.30
Successful Unauthorized System Access by Outsider:.	1.00
Non-disaster downtime:	0.20
Fire:	0.30
Earthquake:	0.30

Data/Information: Other

For threat:

Power loss:	0.20
Communication Loss:	0.10
Data Integrity Loss:	0.70
Accidental Errors:	0.50

Computer Virus:	0.60
Abuse of Access Privileges by Employees:	0.30
Natural disasters:	0.50
Attempted Unauthorized System Access by Outsider:	1.00
Theft or Destruction of Computing Resource:	0.30
Destruction of Data:	1.00
Abuse of Access Privileges by Other Authorized User:	0.30
Successful Unauthorized System Access by Outsider:	0.80
Non-disaster downtime:	0.20
Fire:	0.30
Earthquake:	0.30

Other:Facilities

For threat:

Power loss:	0.20
Communication Loss:	0.00
Data Integrity Loss:	0.00
Accidental Errors:	0.50
Computer Virus:	0.00
Abuse of Access Privileges by Employees:	0.10
Natural disasters:	0.50
Attempted Unauthorized System Access by Outsider:	0.10
Theft or Destruction of Computing Resource:	0.20
Destruction of Data:	0.00
Abuse of Access Privileges by Other Authorized User:	0.00
Successful Unauthorized System Access by Outsider:	0.30
Non-disaster downtime:	0.10
Fire:	0.30
Earthquake:	0.30

Other: Supplies

For threat:

Power loss:	0.00
Communication Loss:	0.05
Data Integrity Loss:	0.00
Accidental Errors:	0.10
Computer Virus:	0.00
Abuse of Access Privileges by Employees:	0.08
Natural disasters:	0.50
Attempted Unauthorized System Access by Outsider:	0.07
Theft or Destruction of Computing Resource:	0.20
Destruction of Data:	0.00
Abuse of Access Privileges by Other Authorized User:	0.30

Successful Unauthorized System Access by Outsider:	0.20
Non-disaster downtime:	0.00
Fire:	0.30
Earthquake:	0.30

Other: Documentation

For threat:

Power loss:	0.00
Communication Loss:	0.50
Data Integrity Loss:	0.00
Accidental Errors:	0.11
Computer Virus:	0.00
Abuse of Access Privileges by Employees:	0.10
Natural disasters:	0.50
Attempted Unauthorized System Access by Outsider:	0.00
Theft or Destruction of Computing Resource:	0.20
Destruction of Data:	0.00
Abuse of Access Privileges by Other Authorized User:	0.00
Successful Unauthorized System Access by Outsider:	0.10
Non-disaster downtime:	0.10
Fire:	0.30
Earthquake:	0.30

Other: Personnel:

For threat:

Power loss:	0.10
Communication Loss:	0.10
Data Integrity Loss:	0.00
Accidental Errors:	0.10
Computer Virus:	0.00
Abuse of Access Privileges by Employees:	0.30
Natural disasters:	0.50
Attempted Unauthorized System Access by Outsider:	0.00
Theft or Destruction of Computing Resource:	0.00
Destruction of Data:	0.00
Abuse of Access Privileges by Other Authorized User:	0.30
Successful Unauthorized System Access by Outsider:	0.30
Non-disaster downtime:	0.10
Fire:	0.30
Earthquake:	0.30

A Method for Quantitative Risk Analysis

James W. Meritt

Jim.Meritt@Wang.com

(703) 827-3534

Abstract

There are two primary methods of risk analysis:

- ***Qualitative*** - Improve awareness of Information Systems security problems and the posture of the system being analyzed.
- ***Quantitative*** - Identification of where security controls should be implemented and the cost envelope within which they should be implemented.

These may be combined into a third:

- ***Hybrid method*** - A selected combination of these two methods can be used to implement the components utilizing available information while minimizing the metrics to be collected and calculated. It is less numerically intensive (and less expensive) than an in-depth exhaustive analysis.

WANG GLOBAL

Scope Statement

The scope statement is your first step. This single statement is what you will give to the Information Technology Committee meeting recorder or incorporate into the submitted proposal. The scope statement MUST must be committed to by all concerned.

The scope statement must:

a. Specify exactly what is to be evaluated

b. State what kind of risk analysis will be performed

c. Provide the expected results

Asset Pricing

As the next step, the information system specified in the scope statement will be broken down into its components which will then be individually priced. While it is possible to break the system down into functional units, I find it much easier to disassemble the overall system into its tangible components which may be more easily priced.

Risks

A *risk* to the information system is something that can, in some way, cause harm or reduce the operational utility of the system. *Threats* are those things which may occur independent of the system under consideration and which may pose the risk.

Exposure/Impact coefficient

All assets are not equally vulnerable to every risk. The degree to which an identified asset is vulnerable to a specified risk may vary from totally invulnerable (example: cabling systems are reasonably invulnerable to computer virus infections) to absolutely destroyed (example: printers, once they are stolen, result in a total loss).

While the possibility of a particular threat of occurring don't change regardless of the controls implemented for the system, the degree to which the system is vulnerable to the threat may be reduced. This is the value which may be modified to compensate for already-implemented controls.

Single Loss Expectancy

Different assets respond differently to different realized threats. The effectiveness of particular threats against varying assets are different from "no impact" to "total replacement necessary" depending upon the sensitivity of the asset and threat under consideration. What follows is a first-order evaluation of this sensitivity. The threats considered are REALIZED - they are assumed to have occurred. The likelihood of a particular threat occurring is considered separately and will not be contained within this evaluation. The SLE (single loss expectancy) is given as a value between 0 and 1 and represents the damage to the asset.

Group Evaluation

The next step involves a group meeting that should be composed of the stakeholders (those with a vested interest) of the system. This meeting should include individuals who have knowledge of the various components in, threats to and vulnerabilities of the system as well as management and operation responsibilities to help in the determination of overall acceptability. This structured meeting is greatly like that advanced by the hybrid facilitated risk analysis methodology developed initially by the Computer Science Institute.

Group Evaluation
(continued)

The meeting provides a common focus on the methodology among the various stakeholders and business units. It is up to you to maintain an open and balanced flow through the meeting by providing clearly defined roles and responsibilities for the various members and to identify or verify:

a. Assets

b. Risks

c. Exposure/Impact

d. Acceptability determination

Calculation

The values were entered into a simple spreadsheet which contained the assets on one axis, the threats on the other and the vulnerability coefficient at their intersection. The second sheet contained a table with similar threat and asset values, but the intersection points were the product of the particular asset times the probability of the threat times the vulnerability of that specific asset to that specific threat.

Value	Risk [1]	Power Loss	Communication Loss	Data Integrity Loss	Accidental Errors	Computer Virus	Abuse of Access Privledges by Em	Natural Disasters [2]	Attempted Unauthorized System Ac	Theft or Destruction of Computing F	Destruction of Data	Abuse of Access Privledges by Oth	Successful Unauthorized System A	Non-disaster Downtime [3]	Fire	Earthquake
		2.00	2.00	2.00	0.72	0.68	0.40	0.29	0.27	0.24	0.17	0.09	0.08	0.06	0.01	0.01
$86,032.25		0.20	0.40	0.00	0.10	0.30	0.10	0.50	0.20	1.00	0.00	0.00	0.10	0.20	0.30	0.30
$185,541.50		0.40	0.50	0.10	0.10	0.10	0.20	0.50	0.10	1.00	0.10	0.00	0.20	0.10	0.30	0.30
$1,440.00		0.10	0.10	0.00	0.30	0.00	0.50	0.50	0.50	1.00	0.00	0.00	0.50	0.10	0.30	0.30
$968,990.61		0.20	0.10	0.00	0.20	0.00	0.30	0.50	0.00	1.00	0.00	0.00	0.20	0.10	0.30	0.30
$909,081.23		0.20	0.10	0.00	0.10	0.80	0.20	0.50	1.00	1.00	0.00	0.00	0.60	0.05	0.30	0.30
$98,181,834.03		0.10	0.10	0.00	0.40	0.30	0.20	0.50	0.30	1.00	0.00	0.00	0.60	0.20	0.30	0.30
$59,651.00		0.10	0.10	0.00	0.10	0.20	0.20	0.50	1.00	1.00	0.00	0.00	0.20	0.20	0.30	0.30
$119,096.04		0.00	0.00	0.00	0.10	0.00	0.00	0.50	0.00	1.00	0.00	0.00	0.10	0.00	0.30	0.30
$9,650,756.69		0.20	0.20	0.00	0.70	0.50	0.40	0.50	0.20	1.00	0.00	0.00	0.80	0.20	0.30	0.30
$121,153.47		0.10	0.10	0.00	0.10	0.05	0.10	0.50	0.10	1.00	0.00	0.00	0.15	0.05	0.30	0.30
$2,282,017.09		0.20	0.10	0.00	0.20	0.30	0.10	0.50	0.10	1.00	0.00	0.00	0.30	0.20	0.30	0.30
$103,062.00		0.20	0.06	0.97	0.50	0.95	0.30	0.50	1.00	0.02	1.00	0.30	0.70	0.20	0.30	0.30
$668,000.00		0.10	0.30	0.70	0.50	0.30	0.50	0.50	0.30	0.40	1.00	0.30	1.00	0.20	0.30	0.30
$0.00		0.20	0.10	0.70	0.50	0.60	0.30	0.50	1.00	0.30	1.00	0.30	0.80	0.20	0.30	0.30
$5,032,233.30		0.20	0.00	0.00	0.50	0.00	0.10	0.50	0.10	0.20	0.00	0.00	0.30	0.10	0.30	0.30
$136,362.18		0.00	0.05	0.00	0.10	0.00	0.08	0.50	0.07	0.20	0.00	0.30	0.20	0.00	0.30	0.30
$8,485,920.00		0.00	0.50	0.00	0.11	0.00	0.10	0.50	0.00	0.20	0.00	0.00	0.10	0.10	0.30	0.30
$18,598,509.00		0.10	0.10	0.00	0.10	0.00	0.30	0.50	0.00	0.00	0.00	0.30	0.30	0.10	0.30	0.30
$145,589,680.39																

Losses: Asset/ Risk	Power Loss	Communication Loss	Data Integrity Loss	Accidental Errors	Computer Virus	Abuse of Access Privledges by Employees	Natural Disasters	Attempted Unauthorized System Access by Outsider	Theft or Destruction of Computing Resource	Destruction of Data	Abuse of Access Privledges by Other Authorized User
Network: modems	$34,412.90	$68,825.80	$0.00	$6,194.32	$17,550.58	$3,441.29	$12,474.68	$4,645.74	$20,647.74	$0.00	$0.00
Network:Routers	$148,433.20	$185,541.50	$37,108.30	$13,358.99	$12,616.82	$14,843.32	$26,903.52	$5,009.62	$44,529.96	$3,154.21	$0.00
Network:Cabling	$288.00	$288.00	$0.00	$311.04	$0.00	$288.00	$208.80	$194.40	$345.60	$0.00	$0.00
Network:Other	$387,596.24	$193,798.12	$0.00	$139,534.65	$0.00	$116,278.87	$140,503.64	$0.00	$232,557.75	$0.00	$0.00
Software:OS	$363,632.49	$181,816.25	$0.00	$65,453.85	$494,540.19	$72,726.50	$131,816.78	$245,451.93	$218,179.50	$0.00	$0.00
Software:Applications	$19,636,366.81	$19,636,366.81	$0.00	$28,276,368.20	$20,029,094.14	$7,854,546.72	$14,236,365.93	$7,952,728.56	$23,563,640.17	$0.00	$0.00
Software:Other	$11,930.20	$11,930.20	$0.00	$4,294.87	$8,112.54	$4,772.08	$8,649.40	$16,105.77	$14,316.24	$0.00	$0.00
EQ:Monitors	$0.00	$0.00	$0.00	$8,574.91	$0.00	$0.00	$17,268.93	$0.00	$28,583.05	$0.00	$0.00
EQ:Computers	$3,860,302.68	$3,860,302.68	$0.00	$4,863,981.37	$3,281,257.27	$1,544,121.07	$1,399,359.72	$521,140.86	$2,316,181.61	$0.00	$0.00
EQ:Printers	$24,230.69	$24,230.69	$0.00	$8,723.05	$4,119.22	$4,846.14	$17,567.25	$3,271.14	$29,076.83	$0.00	$0.00
EQ:Other	$912,806.84	$456,403.42	$0.00	$328,610.46	$465,531.49	$91,280.68	$330,892.48	$61,614.46	$547,684.10	$0.00	$0.00
INFO:System	$41,224.80	$12,367.44	$199,940.28	$37,102.32	$66,578.05	$12,367.44	$14,943.99	$27,826.74	$494.70	$17,520.54	$2,782.67
INFO:Business	$133,600.00	$400,800.00	$935,200.00	$240,480.00	$136,272.00	$133,600.00	$96,860.00	$54,108.00	$64,128.00	$113,560.00	$18,036.00
INFO:Other	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
Other:Facilities	$2,012,893.32	$0.00	$0.00	$1,811,603.99	$0.00	$201,289.33	$729,673.83	$135,870.30	$241,547.20	$0.00	$0.00
Other:Supplies	$0.00	$13,636.22	$0.00	$9,818.08	$0.00	$4,363.59	$19,772.52	$2,577.25	$6,545.38	$0.00	$3,681.78
Other:Documentation	$0.00	$8,485,920.00	$0.00	$672,084.86	$0.00	$339,436.80	$1,230,458.40	$0.00	$407,324.16	$0.00	$0.00
Other:Personnel	$3,719,701.80	$3,719,701.80	$0.00	$1,339,092.65	$0.00	$2,231,821.08	$2,696,783.81	$0.00	$0.00	$0.00	$502,159.74
Total for Identified Ris	$31,287,419.97	$37,251,928.92	$1,172,248.58	$37,825,587.61	$24,515,672.30	$12,630,022.92	$21,110,503.66	$9,030,544.77	$27,735,781.98	$134,234.75	$526,660.20

Analysis

- *Across asset* - A sum of the product of terms was made across each asset for all threats. This summation gives the expected annual loss to that asset for all threats. Looking across these terms will show you which assets need the most protection (the most can be lost there).
- *Across risk* - A sum of the product of terms was made across each threat for all assets. This summation gives the expected annual loss due to that threat to the entire system. Looking across these terms will show you what threats need to be guarded most against (the most can be lost to them)

The sum of all the values in the first should be the same as the sum of all values in the second. This value is the **A**nnual **L**oss **E**xpectancy (ALE) for the entire system to all threats.

WANG GLOBAL

Controls

Controls are those things which are implemented to prevent the exposure to the threat in the first place, detect if the threat has been realized against the system, mitigate the impact of the threat against the system or to recover/restore the system.

Analyze Controls

The controls, once the candidates have been identified or discarded by the group meeting, must be analyzed. Two recommended methods are:

Cost/Benefit ratio - Where the reduction in the ALE when applying the particular control across all assets and all threats is compared to the local cost for implementing the control.

Risks/Control (e.g. "bang per buck") - Where the risks reduced by the control are enumerated (either by count or summed ALE reduction) are compared to the control (either unity or implementation cost).

Conclusion

It is possible to answer management's questions which inevitably turn to costs and other metrics. While there are a number of intangible assets and unquantifiable risks, it is possible to perform some basic mathematical calculations yielding results which may give firm guidance towards improving the security of any system.