Risk analysis in the 1980's

by JEROME LOBEL
Honeywell Information Systems, Inc.
Phoenix, Arizona

INTRODUCTION

The application of scientific procedures to the study and evaluation of information and communications systems risks is still in its infancy. Hopefully, before the end of this decade we will see major breakthroughs both in improved techniques and greater utilization of Risk Analysis procedures by computer users. On the other hand Risk Analysis (also sometimes called Threat or Vulnerability Analysis) has real merit even by todays standards. The problem is that many organizations have still to be convinced as to its potential.

THE PAST—RISK ANALYSIS LIMITATIONS

Risk Analysis attained a certain degree of popularity as a result of a report written for the Federal Information Processing Standards Task Group 15, Computer Systems Security, of the United States Department of Commerce National Bureau of Standards in 1975.

Although recognized as a potentially valuable evaluation tool authorities generally did not present it as a panacea for relieving the ills of an electronic data processing system. Typical systems problems such as fraud, theft, embezzlement, malicious damage, unauthorized access, natural disaster, accident, or an operations interruption or stoppage were considered to be too complex to be resolved by relatively simple mathematical or statistical solutions.

Other criticisms of Risk Analysis methodology included:

- The owners and users of information systems (the people from whom survey data is usually obtained) often do not have enough detailed knowledge as to how their systems work or where their systems work or where their vulnerabilities are located to provide adequate or sufficiently accurate information.
- It is difficult if not impossible (or impractical) to survey 100 percent of an exhaustive list of system vulnerabilities.
- Estimates of event occurrence (the probability of an event occurring) or its cost may be too imprecise to be reliable.
- Some information system threats are not quantifiable in monetary terms (i.e. national security information compromises, loss of public services, etc.).
- The most fallible part of most information systems, the human factor, is too unpredictable and uncontrollable to measure.

In spite of these limitations, many organizations began to use Risk Analysis or some variation of it to get a better "handle" on their information system vulnerabilities.

THE PRESENT—STANDARD PROCEDURES

In practice, there are many variations in Risk Analysis technique and approaches. The basic process of Risk Analysis however tends to follow the following four steps:

1. A survey is made of an organization's risks associated with its most essential assets, typically its people, information and facilities. Normally the data gathered during the survey or study includes:
   - The identification of potentially injurious or disastrous events,
   - Estimates of the frequency of occurrence associated with risk events (Figure 1).
   - Estimates of cost (usually in money) of the loss per incident of event occurrence (Figure 2).

   Special statistical tables are often used to permit even gross estimates of time or cost to be mathematically useful.
2. Calculations are made based upon the input data (estimates made during the survey) and result in the derivation of an expected *annual loss* from the occurrence of a particular event (Figure 3).
3. A detailed evaluation of each event or problem area is made to identify the best known preventative measures and their associated costs.
4. A return-on-investment (ROI), pay back calculation or other comparative measurement technique is used to evaluate the reasonableness of spending time, money or energy to reduce a particular risk. Risk Analysis studies usually result in some form of management decision. As an example, if a particular risk prevention measure is deemed too expensive or not practical, a decision may be made to "tolerate" the risk.

Advocates claim that the final result of a formal Risk

				E/Y = FREQUENCY OF EVENT	
				P = PROBABILITY	
EXAMPLE:					
LET P	=	0	IF PRACTICALLY NEVER		
	=	1	IF ONCE IN 300 YEARS		
	=	2	IF	" "	30 YEARS
	=	3	IF	" "	3 YEARS
	=	4	IF	" "	100 DAYS
	=	5	IF	" "	10 DAYS
	=	6	IF	" "	1/DAY
	=	7	IF		10/DAY
	=	8	IF		100/DAY
(IF 3 YEARS = 1000 DAYS)					

Figure 1—Probability of frequency estimation table.

EXAMPLE:				
LET COST	=	12	IF LOSS IS	$ 3,333,333
	=	11	" " "	$ 1,000,000
	=	10	" " "	$ 333,333
	=	9	" " "	$ 100,000
	=	8	" " "	$ 33,333
	=	7	" " "	$ 10,000
	=	6	" " "	$ 3,333
	=	5	" " "	$ 1,000
	=	4	" " "	$ 333
	=	3	" " "	$ 100
	=	2	" " "	$ 33
	=	1	" " "	$ 10
	=	0	" " "	$ 3
				L/E = LOSS PER EVENT

Figure 2—Estimate of order of magnitude table.

Analysis survey will be a set of informed management decisions, possibly several magnitudes better than the intuitive guess-work that might have otherwise taken place. It is also proposed that Risk Analysis should be a dynamic or on-going process which is repeated or periodically updated. Its advocates also claim that it is one of the few systematic approaches to resolving potentially dangerous problems associated with certain data processing and communications systems.

Risk Analysis studies may be performed by special data processing project teams, internal audit staffs, professional security staffs or outside consultants, just to name a few of the organizations often called upon to do the job.

THE FUTURE—TAILORING PROCEDURES TO SATISFY REAL WORLD NEEDS

The idea that Risk Analysis, as a way of measuring and correcting information system threats, might be overlooked by computer users led to a survey of 250 organizations that had already been exposed to the methodology. The objective of the survey was to analyze the extent to which formal Risk Analysis procedures were being used by these organizations and the nature of the benefits that were being derived. Fifty-eight responses were received and were tabulated in the results.

Altogether, there were ten questions in the survey. A number of the questions had multiple parts and permitted the respondee to comment on significant issues. All responses were based upon organizational as opposed to individual experiences.

The following is a list of the questions, the responses tabulated, and this author's comments and conclusions regarding the response to each question:

1. Has your organization implemented a formal Information Systems Risk Analysis program at any time?
   Response: Yes = 10 No = 48
   Comment: The low response of 21 percent (organizations with formal Risk Analysis Programs) indicates that, at the very least, Risk Analysis has not yet met with wide acceptance as a means of identifying and correcting information system threats.
2. Has your organization used the *formal* Risk Analysis technique for studying information system weaknesses at any time in the past?
   Response: Yes = 12 No = 46
   Comment: For those organizations that have im-

EXAMPLE

L/E = EXPECTED LOSS PER EVENT

E/Y = EXPECTED FREQUENCY OF EVENT

L/Y = EXPECTED AVERAGE LOSS PER YEAR

L/Y = (L/E) (E/Y)

Figure 3—Expected average loss per year calculation.

plemented the program, it appears that they must have either attained some degree of success or that the program is only in its initial phase of implementation. (Only one organization indicated the program was a washout.)

3. If your organization has used Risk Analysis, would you say that the extent to which it was applied was:

Response: Check one only

a. Extensive (all or most systems or applications)?	9
b. Moderate (¼ to ½)?	3
c. Occasional (less than ¼)?	10

Comment: Although there appears to be some discrepancy between the answer to this question and the previous questions, it would seem that the majority of organizations that implemented a *formal* Risk Analysis program tended to go all the way—that is surveyed and evaluated all applications as opposed to only part of their information system. (It is likely that organizations that checked part c., "Occasional," probably did not consider their prior use of Risk Analysis type studies as being a "formal" application of the methodology.)

4. If your organization implemented a Risk Analysis program, how good were the results?

Response:

a. Excellent (est. savings in excess of $.5 million)	0
b. Good (est. savings between $100,000 and $.5 million)	2
c. Fair (est. savings less than $100,000)	0
d. Poor (savings could not be identified)	9

Comment: The rather negative outcome indicated by the responses to this question can be indicative of generally poor results, poor follow-up, measurement difficulty, or it may have been too early for Risk Analysis users to measure their results. Also, there were a number of questionnaires sent back with comments to the effect that the reason for their organization doing Risk Analysis was not necessarily to obtain monetary cost savings. They said that their main objective was simply to identify risks and implement preventative measures.

5. If your organization has not used Risk Analysis, which of the following reasons probably accounted for this:

Response:

a. Lack of management support	18
b. Lack of adequate information on the technique	17
c. Technique lacks rigid discipline	2
d. Other techniques easier to use	3
e. Could not determine a Risk Analysis Survey would accomplish anything	13

Comment: The reasons given for not implementing a Risk Analysis program indicate that potential users want a lot more proof that the effort and results will probably be worthwhile. So it seems likely that we will not see a significant increase in the use of formal Risk Analysis programs to reduce information system threats until more organizations report positive results, or possibly develop and use other techniques which get the job done better. There is also a strong indication that many potential users of Risk Analysis are looking for more educational information and articles on Risk Analysis methodology and its practical application.

6. What would you say is the strongest argument for doing a Risk Analysis study?

Response:	Check as Appropriate
a. Quantification of system risks and priorities	30
b. Focus attention on high risk areas	29
c. Confirmation of previous threat studies	2
d. Alerting of the organization	30
e. Management participation	11
f. No other technique available	0
g. The resulting action steps	9

Comment: It is interesting to note that responses to this question indicate a greater interest in the communications and quantification value of risk analysis compared to the final outcome or results of implementing study recommendations. This may mean that many people consider Risk Analysis more of an education and planning tool than the final answer as to where to apply resources to minimize or eliminate information system vulnerabilities.

7. If your organization is not using Risk Analysis techniques, are you using some form of substitute program or procedure?

Response: Yes = 11 No = 27

Comment: The number of yes answers are significant inasmuch as almost as many Risk Analysis-using organizations reported they were using some form of *modified* procedure for evaluating systems risks. (See the next question.)

8. If you have used or are presently using Risk Analysis, have you modified or improved on the standard procedure in order to get better results?

Response: Yes = 10 No = 16

Comment: Again, the large number of organizations that reported that they were using some modified form of Risk Analysis to study their system vulnerabilities seems to attest to the need for organizations to tailor whatever procedure they elect to use to their own needs and purposes.

9. If you have used or are using Risk Analysis, have you developed any new or unique survey forms or cal-

culation procedures that you could share with other interested organizations?

Response: Yes = 5 No = 23

Comment: Although only a few of the responding organizations felt that they were in a position to contribute to the state-of-the-art (at the time of this survey), the ideas that were sent in were extremely interesting. (See the next chapter—Risk Analysis Enhancements.) As an example, a number of organizations went to some form of unique procedure for prioritizing or weighting risks related to the needs of their own organization. This helped to partially reduce the amount of time and precision required to estimate risk relevancy and monetary cost savings. As a result, a Risk Analysis study using an alternate procedure might be more useful to a particular organization. Furthermore, modified approaches probably work better where the inherent nature of the system makes it difficult or impractical to utilize monetary values as a basic measurement criteria.

10. If your organization has not performed a Risk Analysis Survey or other similar study of your information system vulnerabilities, what are the possibilities of a program being implemented sometime in 1979?

Response:		
	Excellent	10
	Probable	19
	Negative	14

Comment: The majority (29) of the responding organizations that had not yet already initiated some form of formal Risk Analysis program indicated that they would probably do so prior to the end of this year (1979). To some extent, this is surprising in the light of the answers given to the other questions in the survey. One conclusion that could be drawn in line with this response is that computer users recognize that systems abuses and risks do not appear to be diminishing, and therefore some type of action program will soon be needed. The problem may be which risk evaluation program should be implemented and when?

RISK ANALYSIS ENHANCEMENTS

Thanks to the generous cooperation of the organizations that responded to the Risk Analysis Survey, the following ideas are presented as examples of techniques that might be used to modify or enhance a Risk Analysis program.

Example 1

Objective: A simpler, less expensive procedure—This computer user reported that they operated a medium-sized installation, and didn't have the manpower to implement a "formal and extensive" Risk Analysis program. Their solution was to develop a simplified data gathering form (Figure 4), which they felt short-cutted a more expensive and time-consuming study.

Example 2

Objective: Shorten the Risk Analysis data gathering cycle and expedite evaluation of more critical computer applications—This organization initially used the evaluation procedure published by the Institute of Internal Auditors in their Systems Auditability and Control-Audit Practices guide. They reported that they didn't have time, however, to compile all of the required data, but determined that they could get by with three indexes and an overall summary. (See Figure 5.) The indexes are referred to as the: (1) Major Systems Index, (2) Company Assets Index, and (3) Critical Systems Index.

Example 3

Objective: Modify standard Risk Analysis procedures to more clearly distinguish the severity of impact of different classes of hazards—This organization developed an eight point "degree of loss" index (See Figure 6), and a special form to permit a more quantitative review of information system hazards.

CRITICAL

COMPUTER SECURITY ANALYSIS
(DATA GATHERING FORM)

System name ______ System Identification ______

Description of system:

← MANUAL SYSTEMS →← COMPUTER SYSTEMS →

Input from							
Output to							

Effect of disruption of service:

Alternate method:

Effect of loss/destruction of files:

	Fire	Power	Earth	Sabotage	Fraud	Error
Probabilities of occurrence						
Recovery plan established						
Countermeasures taken						

Remarks and notes:

	COST OF LOSS	
TYPE OF LOSS	FILES	BUSINESS
PERMANENT		
TEMPORARY		

Figure 4.

RISK IMPACT INDICES

(Critical Scale is 1 to 10 with 10 being the high value or most ciritical condition)

Major Systems Index

9-10	Over 60 programs or 100 man months of maintenance, or 10,000 computer hours annually and updates a major master file and interfaces with another major system.
7-8	35-60 programs or 20-100 man months of maintenance or 1,000-10,000 computer hours annually and updates a master file and interfaces with another system.
5-6	10-34 programs or 10-20 man months of maintenance or 250-5000 computer hours annually.
3-4	5-9 programs or 5-9 man months of maintenance or 50-249 computer hours annually.

2 and below other system

The Company Assets

9-10	Directly affect cash
8	Affects movement of assets
6-7	Indirectly affects movement of assets

5 and below less affect on assets

The Critical System Index

9-10	Necessary to maintain daily business
7-8	Necessary to maintain statutory requirements and monthly reporting
5-6	Necessary to maintain business

4 and below not primary to business

Figure 5.

DEGREE OF LOSS MATRIX

HAZARD: ______ NO. ______ TYPE

DEGREE OF LOSS:	MANIFESTATIONS:	RATINGS LOSS	FREQ.
A. MINOR ANNOYANCE			
B. MAJOR ANNOYANCE			
C. MINOR LOSS/RECOVERY			
D. MAJOR LOSS/RECOVERY			
E. MAJOR INTERRUPTION			
F. SEVERE DISRUPTION			
G. MAJOR DISASTER			

Figure 6.

Example 4

Objective: Modify Risk Analysis procedure to permit an evaluation of risks that do not lend themselves to monetary measurement criteria such as events involving adverse social or political consequences—This organization is experimenting with the coupling of conventional Risk Evaluation Procedures with a unique "sensitivity value" or point scale (Figure 7), in order to measure critical events which do not permit monetary assignments.

SENSITIVITY VALUE SCALE

Sensitivity Value Factor plus Back-up Factor may be used to calculate "Exposure Points Value" per year --

Example

Asset List	Value Points
1. Operators manual	10
2. System reference manuals	50
3. Operational files	100
4. Data Base file	250
5. Program Library	300
ETC.	ETC.

Figure 7.

Example 5

Objective: More clearly distinguish between "major" and "minor" threats and classes of exposure present in an information system—In the interest of simplifying the Risk Analysis procedure and at the same time focus attention on the threats of potentially great severity, this very large computer user developed a unique two-level threat classification system (Figure 8). They also divided potential security exposures into four categories. (Figure 9).

MAJOR/MINOR THREAT CATEGORIES

MAJOR THREATS:	An event of catastrophic proportions which destroys the ADP facility or renders it inoperable. Examples: fire, flood, earthquake, tornado, bombing, riot. Assumption is made that all attendant areas of the facility, such as the tape/disk library, are destroyed. Relocation to an alternate processing site is required. Only the material stored off-site is available for use.
MINOR THREATS:	This category includes all the failures, errors, and mishaps encountered daily. While each occurrence may result in relatively short processing delay or minor distortion or loss of data, the cumulative cost of many occurrences can be significant. Examples: CPU failure, wrong tape or pack mounted, listings lost, air conditioning failure.

Figure 8.

CONCLUSION

It is very difficult to prove that a computer system Risk Analysis study will necessarily result in a more secure in-

SECURITY EXPOSURE IMPACT CLASSIFICATION

	Security Exposure	Possible Results of Security Failure
1.	Data Integrity	*Destruction or unauthorized modification of data,* unintentional or deliberate.
2.	Data Confidentiality	Unauthorized disclosure of sensitive data.
3.	Operational Reliability	Undependable or inadequate processing; unavailability of processing. (Processing should be accurate, dependable, and timely.)
4.	Asset Integrity	Destruction or physical damage to buildings and equipment and supporting functions.

In general, the first three categories represent threats to data and processing. Asset integrity can most often be related to physical assets: equipment, supplies, furniture, storage media, etc.

Figure 9.

formation system. On the other hand, as evidenced by the survey covered in this paper, computer users need a systematic way to study, evaluate and prioritize the risks and countermeasures associated with their systems. Risk Analysis lends itself to this task.

Fortunately, there are many risk investigation methods from which to choose. Different organizations should use the methodology that gets the job done, at a price they can afford to pay. There is no question that data processing users need to become more knowledgeable regarding their system vulnerabilities and risk prevention methods. Therefore, slowly but surely, we will probably see more organizations implementing a risk or threat or vulnerability analysis in one form or another. The procedure used will not be nearly as important as the overall results that will be obtained.

REFERENCES

1. ADP Security Handbook—Handbook Supplement: DIPS Manual Chapter 6, U.S. Department of Agriculture, 1977.
2. Carrol, John M., *Computer Security,* Security World Publishing Company, Inc., 1977.
3. *Computer Security Risk Analysis and Control: A Guide for the DP Manager*—National Computing Centre, Ltd., 1979 (available in the U.S. from Hayden Book Company, Rochelle Park, N.J. 07662).
4. Courtney, R. H., "Security Risk Assessment In Electronic Data Processing Systems," IBM Corp., 1975.
5. "Guidelines for Automatic Data Processing Physical Security and Risk Management," FIPS Publication 31, National Bureau of Standards, June 1974.
6. Koenig, Rick, "How to Get a System Security Project Off the Ground!" *Computer Security and Privacy Symposium Proceedings,* Honeywell Information Systems, 1977.
7. Kraus, Leonard S. and MacGahan, *Computer Fraud and Countermeasures,* Prentice Hall, 1979.
8. Martin, James, *Security, Accuracy, and Privacy On Computer Systems,* Prentice Hall, 1973.