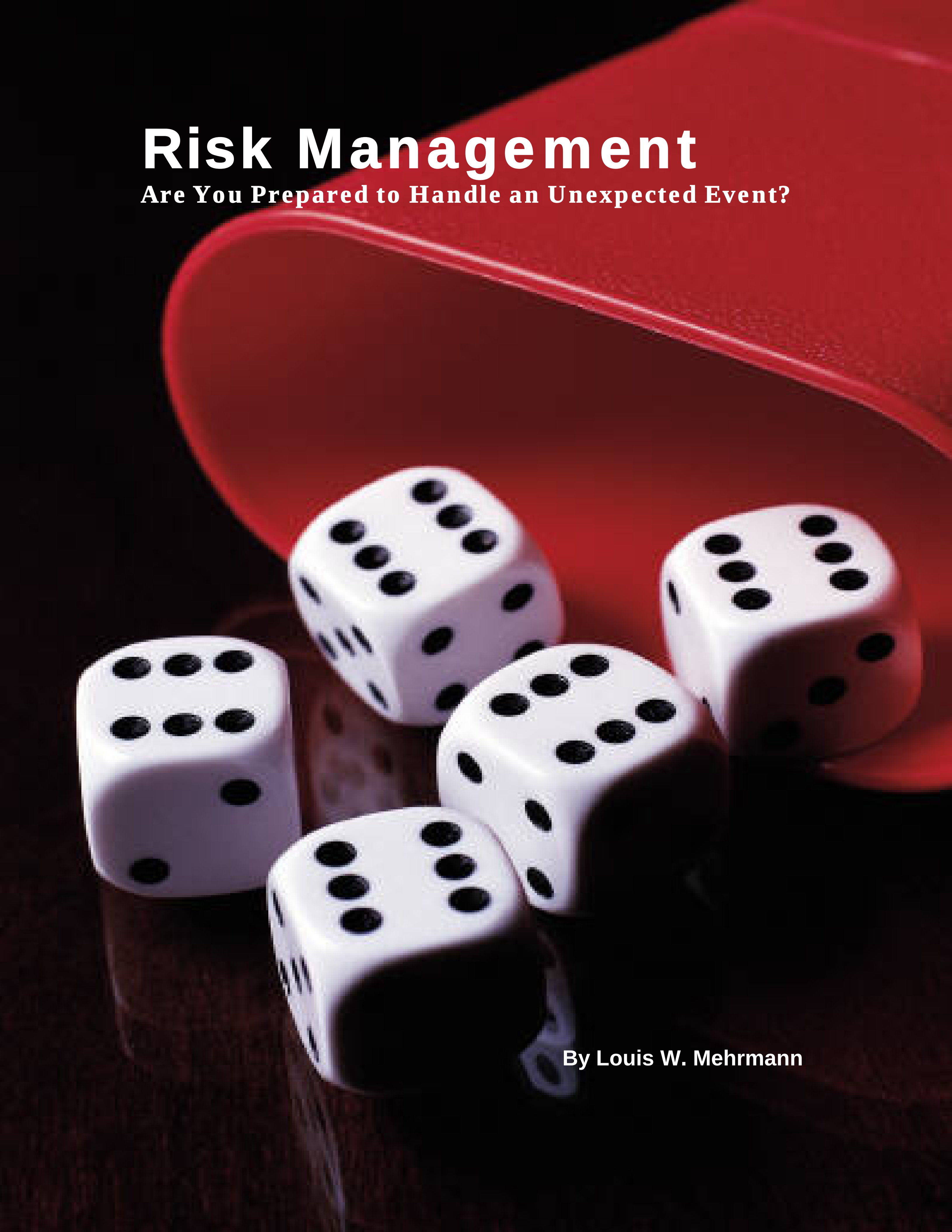
Risk Management

Are You Prepared to Handle an Unexpected Event?



By Louis W. Mehrmann

INDEX

"Identify, Analyze, Qualify, Question, Quantify, Specify, Prepare, Take Protective Action, and Reap the Benefits"

- Anonymous

Risk Management Introduction

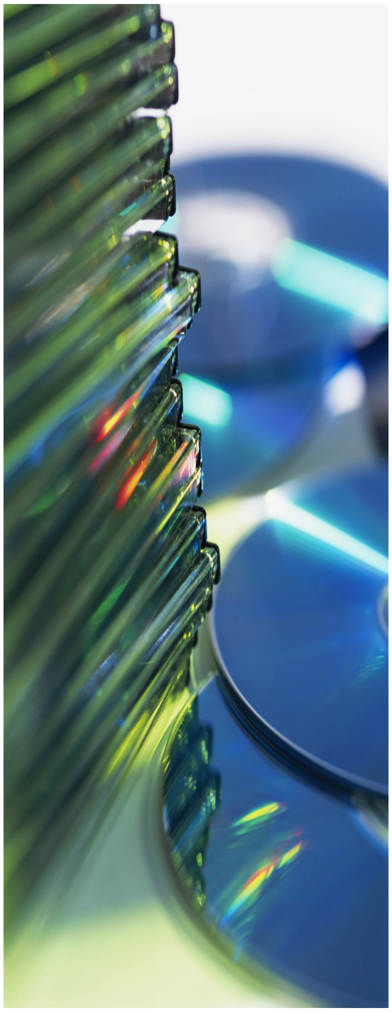
Most management decisions involve the assumption of risk – the chance that things may not turn out the way we hope or want them to.

Are the consequences acceptable?

INTRODUCTION

Decisions made in spite of uncertainties, and in recognition of them, are essential to dynamic, successful management. Most frequently, however, the key to success lies not in the willingness to accept uncertainty, or to assume risk, but in the ability to recognize and quantify the elements of that risk to deal with them in a fully objective way. Virtually every manager must come to grips with and manage risk in some form. For this reason, risk management is an integral part of general organization and project management.

The steadily growing dependence of virtually every kind of organization on electronic information processing systems has introduced new concerns, which themselves have grown rapidly over the years. These concerns are attributable to a wide variety of factors, but there are three principle ones:



- ✓ First is the recognition of the rapid growth in the centralization of the data keeping and information extraction processes with the attendant potential for loss of the entire facility or major portions of it. Such loss might result in a severe setback for the entire organization.

- ✓ Second is recognition of the increasing dependence of the enterprise on employees with skills, talents, and disciplines, and sometimes motivations, quite different from those with which management has been familiar in the past. There is a feeling that these people might present new, unfamiliar problems and unfamiliar problems generally yield more discomfort than do familiar ones.

- ✓ Third is the recognition of an increased proliferation of mini, micro processing devices with an associated distribution of key data to remote intelligent nodes for data extraction, data update and data addition. This new environment, whereby information normally stored in and controlled by the central block-house is now under direct control of a number of remote locations, has led to additional concerns for the protection of data from disclosure, modification, and/or destruction.

ASSESSMENT PROCEDURES:

There is no assertion that the procedure described herein is the only way to do a successful risk assessment. In fact, any procedure that provides sufficient accuracy and credibility while reducing the amount of labor to perform the assessment is acceptable. There are, however, several characteristics of an acceptable procedure. These include the following:

1. **Quantitative results**
   The process must yield Data, describing the cost of potential problems in terms of cost per unit of time, such as dollars per year.

2. **Fundamental Simplicity**
   The process should be readily comprehensible by the highest levels of management expected to support and fund action based on the data it yields.

3. **Usability**
   The requirements for data from the Data Processing facility's users should be sufficiently limited in complexity as to be readily understandable by persons whose areas of competence and interest do not include risk assessment.

Assessment Scope

Initial presentations of the procedures described herein provoked much discussion of the scope and nature of problems considered in performing a risk assessment. Some argued that consideration should be limited to catastrophic events, such as fire, floods, earthquakes, and volcanoes. Others argued that only intentional misconduct such as fraud and embezzlement are relevant.

The correct position is to ***extend consideration to the effects of all of the undesirable things that might happen to data or to the means of accessing and processing data***. Take care here to insist that concern be limited to the *effects* of undesirable things and not be extended to the creation of a virtually endless list of bad things – ***the threats list***. It is, for example, quite possible to consider the *effect* of power failure without completing a list of all things that might cause the power to fail.

There is no basis for the exclusion from consideration in the risk assessment process of any categories of damage or disruption to data processing activities. It is not until the cost of the undesired event and its estimated frequency have both been examined (which is in fact a risk assessment) that a potential source of damage can be justifiably excluded from further consideration.

Assessment Purpose

The purpose of performing a risk assessment is to obtain a quantitative statement of the potential problems to which the data processing facility are exposed. Then appropriate, cost-effective protective safeguards selected. It is assumed that, once armed with information, ***no protective measure will be selected which costs more than the toleration of the problem***. The risk assessment should establish that threshold.

Principal Factors

Analysis Elements

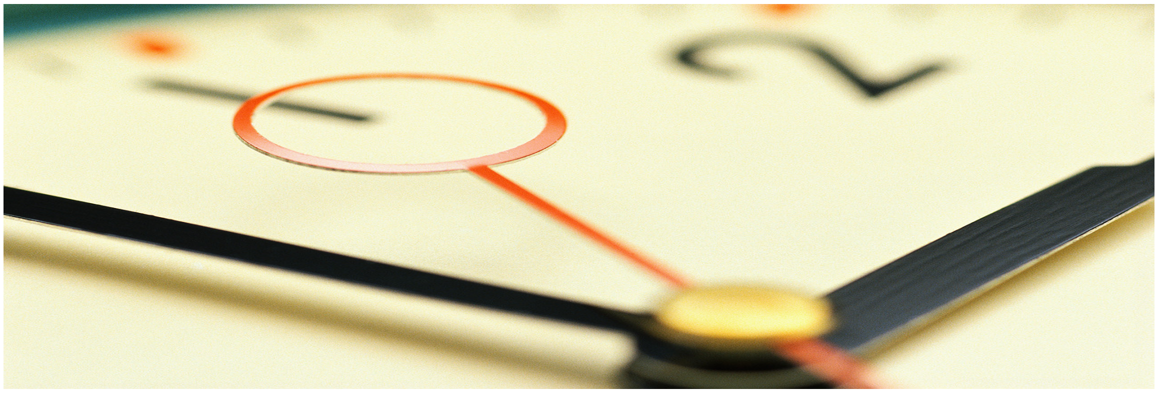
Most people who have seriously considered risk analysis techniques or attempted to devise a risk analysis procedure readily agree that to be useful a technique must yield a quantitative statement of the effect of specific problems. In addition to a measure of the extent of damage, a statement of the probability of occurrence of a particular event is essential to a useful risk assessment. The two key elements in a risk analysis are:

1. **Severity**
   A statement of impact relative to the severity or damage of a specific difficulty if it occurs

2. **Frequency**
   A statement of the probability of encountering that difficulty within a specified time period

It is necessary to define both parameters to describe risk in terms of cost per unit time, such as dollars per year.

The probability of an undesirable thing happening is usually more difficult to determine with confidence than is a measure of the consequence of its happening. We are so accustomed to making unconscious, gross, subjective judgments of probability in reaching decisions that it is difficult to accept a formalization of the process. Whatever the reasons for finding it difficult, statements of the potential economic effects of events without regard to their relative probability cannot lead to the identification of those harmful exposures that are worthy of corrective action versus those which are not.



Risk Options

There are many events which could have catastrophic consequences but which appear to have such a low probability of happening that the expenditure of significant resource to lessen the potential damage is not justified. For example, a number of years ago, we judged the probability of nuclear attack to be sufficiently high enough that authorities persuaded families to build and stock fallout shelters. We have now, for the most part, abandoned those shelters or converted them to some other purpose, not because the damage caused by such an attack is less, but because we judge the probability of such an attack to be too low to justify the cost and inconvenience of maintaining these facilities. The decision to abandon this protective measure was based on a reassessment of he probability of occurrence – not on change in the consequences if it happened.

As another example, assume that a hypothetical major corporation has centralized most of its data processing facilities into a single location. Also, assume that no plans exist for data processing support elsewhere in the event of a catastrophic loss of that facility. Suppose that the sum of all costs to the corporation of such a loss is $150 million, including not just the replacement costs of hardware, but also lost business opportunities, lost customers, interruption of proper cash management, and other key activities. As such, knowledge of the $150 million figure, by itself, does not lead itself to any real measure of the problem. It does not suggest how much to spend to reduce the exposure. If, through further analysis, it is determined that we might reasonably expect such a loss with a frequency of .003/year, we have some basis for a corrective action decision. Based on this information, the exposure definition is in the order of $450,000 per year.

Continuing this example, we have three options to address the exposure.

1. Tolerate it.
2. Lower potential cost by implementing measures costing less than a total of $450,000 per year.
3. Lower the probability of loss occurring by implementing protective measures costing less than the exposure.

The point is that, unless we had quantified both the potential cost and the probability of occurrence, we would not be in a position to make an informed election of any of the three options.

Other words and phrases are defined
bold type when used.

D. "Bodily injury" means bodily harm, si
disease, including death that results.

E. "Business" includes trade, profess
pation

Insurance as an Option

Parenthetically, we should note that insurance is not a fourth option. Insurance provides a means of smoothing the effect of the loss when and if it happens. As such, it is a matter considered after the election of the other options. The availability of insurance does not lessen the desirability of minimizing risk by other measures. Downward adjustment of risk should lessen either:

- ✓ The amount of insurance required (in case of reduced cost) or
- ✓ The insurance rate (in case of reduced probability of occurrence)

In the unlikely event that risk reductions will not change the cost of insurance, this affects the decision to insure or the decision to apply protective measures.

Evaluating Sensitive Data

There are many ways to measure the impact of security risk, one of which is dollars and cents. Those who seem to have the most difficulty in assigning dollar values to security problems are, for the most part either:

- Considering the safety of data collections that, if disclosed or otherwise harmed, would have some identifiable and undesirable political or social ramifications, and are possibly affected by privacy legislation

- Involved with Defense or Intelligence activities

The risks associated with activities in these two categories are generally much more difficult to assess quantitatively than are many other exposures. However, this does not lessen the desirability of such assessment.

The reluctance to use dollars as a means of sizing the negative social impact of security problems is understandable. We must anticipate that many people will not look kindly on those who appear to assess in dollars the damage that might befall people as consequence of some security problem. The appearance of measurement in dollars, for example, of an individual's privacy concerns might be abhorrent to some people.

This reluctance to use dollars as the measure has led to several parallel development efforts to define the severity of problems in these categories using relative sensitivities as, for example on a scale of 1 to 5. Such rating schemes are valuable and should be encouraged. They are a means of communicating an assessment of the potential harm to people from the loss of security to files of specific types.

For example, a rating of "1" indicates great sensitivity for psychiatric data and "2" for files containing less sensitive data such as tax files. However, these ratings do not provide an adequate parameter for guidance in selecting economically feasible security measures. Such rating schemes can and should coexist with risk analysis techniques that quantify the problem in dollars.

It is conceivable to couple a convention using relative sensitivities on a scale of 1 to 5 with another describing probability of occurrence to provide an expression that results in, "the probability of a 2 sized problem is 0.3/year". However, this does not provide much help in evaluating the need for, or relative effectiveness of, specific security measures.

Justifying Security

A specific security measure to contain only one problem is often difficult to justify. The best security measures usually contain or assist in containing multiple problems.

Any summation of risks contained by a specific or combinations of specific security measures requires expressing the risks in ‘common units of measure’. If some problems are expressed in economic terms and others in non-dimensional sensitivity ratings, the ability of specific measures to contain this variety of problems will be awkward to assess and difficult to cost justify.

Much of the problem of quantifying subjective concerns often goes away if, in performing the risk analysis, we defer until last the decisions we do not know how to make. Frequently other, more easily quantifiable concerns fully justify the required security enhancement.

As an example, it is usually difficult to derive a quantitative statement of the effect of an exposure of the violations records associated with vehicle operators’ license files. That such data is generally public record does not lessen belief that consolidation of such sensitive data results in potential for exposure to too many people who should not have access to see them. However, the need to protect such data against unauthorized, accidental or intentional (illegal) modification should justify a level of security sufficiently high enough to displace concerns for disclosure as the dominant factor in selecting security measures. In this manner, it is reasonable to justify adequate protection without the need for exposure quantification.

Serendipity will always prevail in such matters, but there is no reason to ignore any assistance that it might provide. Experience indicates that the application of standard risk analysis methodologies to data collections will often dictate measures adequate to include protection against disclosure and thus relieve the need for solid quantification of the social impact, real or imagined.

While those considering the problem of the social impact of losses of data security have trouble expressing in dollars the damage which might be done to people, the defense establishments have a greater problem in addressing the other factor in the risk analysis expression, the probability of occurrence.

It is not easy to assess the dollar implication of losses of classified data or denial of processing capability. It is an even greater problem when trying to assess the probability of espionage and sabotage. Because the losses in such cases can be very great, it becomes difficult to accept as tolerable any probability of occurrence. This dilemma leads to such logical dead ends as the statement that "if it can happen, we must assume that it will happen with a probability of 1".

There is no basis for the assignment of specific values to the probability of espionage or other illegal conduct relative to the security of military or intelligence data. However, this does not justify the assumption of meaningless extremes. The result of assumptions is often irrational or, at best, highly subjective response to the problem.

The use of electronic data processing capabilities in the handling of classified data has complicated security more by introducing problems than by increasing the actual severity of the problems. Most approaches to protect classified data, with a few notable exceptions, are wholly pragmatic and based on simple "reasonable person" criteria. The level of interference that the operation can tolerate is most often the criteria for selection and application. This does not suggest that such criteria are wrong. It may be the only way when it is impossible to define the possibilities adequately. It is necessary to remember the workability of this approach when first considering security in data processing operations involving classified data.

It is also important to avoid the inclination to overemphasize the significance of technical problems simply because their solutions are intellectually challenging. Frequently, the more intellectually stimulating problems are also those with low probabilities of occurrence. The probability of occurrence of these more exotic problems is lower by the limited number of people in a position to pose each specific problem. We are more inclined to be concerned for the potential damage by a system programmer. Although there are few programmers, their capabilities provide quite challenging problems. We are less inclined to conduct a critical evaluation of the effectiveness of guards keeping strangers, of whom there are many, out of a facility and in restraining persons from carrying out what they should not remove from the premises, including media for data storage.

Fortunately, the great majority of systems in both government and private sectors do not have security needs dominated by unquestionable events or probabilities of occurrence due to undefined potential social impact or defense problems. Even in systems free of these problems, it may at times be difficult to arrive at precise assessments of event impact or probability. It is usually quite feasible to arrive at figures that, while inexact, are good enough to evaluate exposures and provide guidance in selecting appropriate security measures.

Methodology

Assessment Objectives

The objective of a risk assessment in the Electronic Data Processing **(EDP)** area is a quantitative statement of the potential cost of losses of security in and about a data processing facility where such losses might result in a failure to provide the services desired or expected of that facility. The goal which this objective supports is the implementation of controls which, costing significantly less than suffering the problems to which they apply, bring the associated EDP operations risk to an acceptable level.

It is important to recognize that the goal is to protect 'the provision of EDP services' through 'protection of the capabilities' needed to provide those services. Thus, we are concerned with the protection of means of capabilities – not physical assets.

Some of he means or capabilities on which there may be heavy dependence for successful EDP operations may not be assets of the organization under consideration. They may be the property of a communications common carrier, a software licensor, or leased hardware. Again, the emphasis here must be on protection of EDP capabilities to assure continued provision of services of a quality adequate to the needs of the facility's users. In this context, capabilities include all of those things needed to provide those services, including hardware, programs, data, people, physical space, communications, power, and environmental controls.

In the output of an EDP risk assessment, the importance of a resource reflects in its significance to the function supported by the EDP facility under consideration. The more critical any function is to the well being of the organization, the greater the importance of the resources needed to provide support to that function. The evaluation process should identify and prioritize:

- **All critical functions supported by the EDP facility**
- **The critical resources required to support provision of those critical functions**

Problem Sources

Data security problems are those presented by any of the six undesirable things that could happen to data. They are:

1. **Accidental Disclosure**
2. **Accidental Modification**
3. **Accidental Destruction**
4. **Intentional Disclosure**
5. **Intentional Modification**
6. **Intentional Destruction**

In addition, there can be the denial of processing capability.

It is important to keep all of the undesired items in mind because protective measures, to be fully cost-effective, need to address the broadest possible array of problems. If attention converges on too narrow a definition of data security, it is quite possible that a set of protective measures could be selected which contain a smaller problem scope than other measures that could be selected with the broader problem definition in mind.

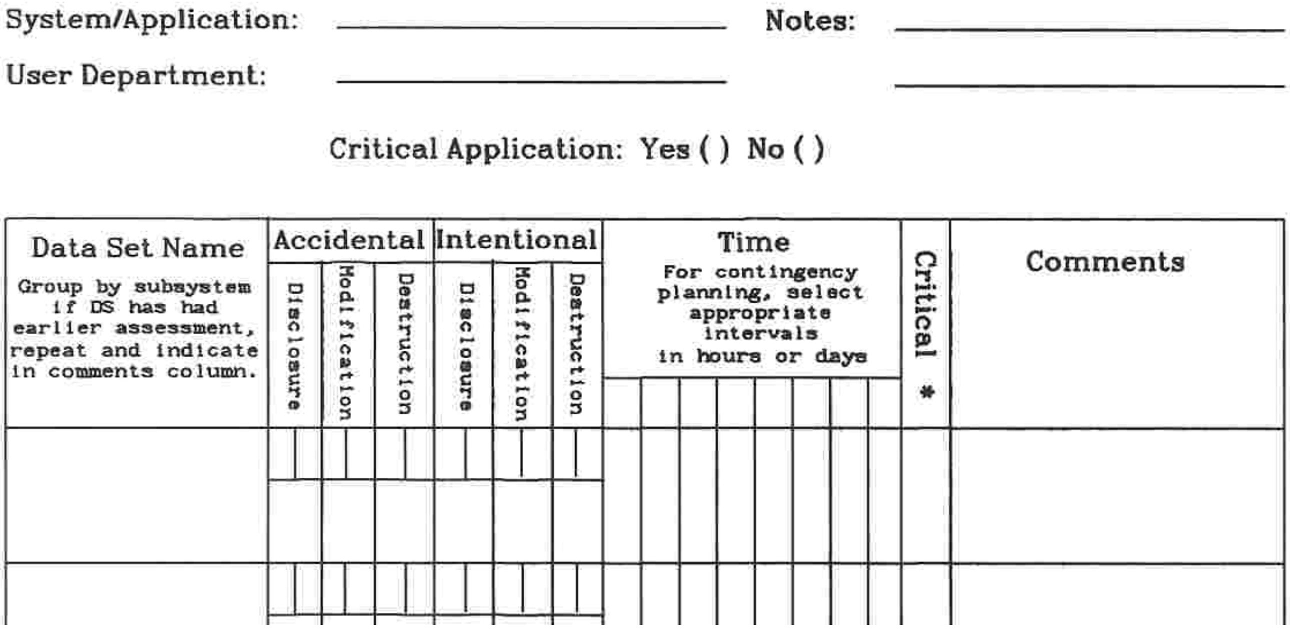
The probability of occurrence may vary widely as a function of which data is considered. Experience has shown it to be desirable to look at the potential cost of an event and its probability of occurrence in a rather fine-grained structure. That is, to look at the results of each bad thing happening to every file, dataset, or other convenient aggregation.

The selection of appropriate protective measures is highly dependent upon the specific problem to be contained. If our problem structure is too coarse, combining the consequences of both accidental and intentional things, the result will not usually provide the desired guidance to select a set of cost-effective protective measures.

Risk Analysis Form

This sample form evaluates the risk of damage to data from all causes, including the loss to physical threats, such as fire.

The form forces the examination of the consequences of security problems to the data set level, the data sets listed are in groups by each application. The risk assessment is at the application level, not at the data set level.



System/Application: ______________________ Notes: ______________________

User Department: ______________________ ______________________

Critical Application: Yes ( ) No ( )

Data Set Name Group by subsystem if DS has had earlier assessment, repeat and indicate in comments column.	Accidental			Intentional			Time For contingency planning, select appropriate intervals in hours or days	Critical *	Comments
	Disclosure	Modification	Destruction	Disclosure	Modification	Destruction			

(Sample Risk Analysis Form)

Doing a Risk Analysis

Refer to the format of the Sample Risk Analysis form. The far left column is for listing the data collections needed to support the application under consideration. If this application is easier to consider with further subdivision, group the datasets accordingly. However, do not force further subdivision if not necessary.

“Unless it is readily done, it should not be done”

Some datasets support more than one application. In such cases, it is necessary to list them with each corresponding application and make a notation in the comments column that they are on the list in this manner. It is not satisfactory to list only once those files that support several applications because some applications may be more dependent on that dataset than other applications. Further, unless a file is on the list with each corresponding application, the totality of the dependence may not be calculable.

The first objective is to assign values for impact (V), frequency (P), and annualized risk cost (E), at each intersection in the matrix below.

	P = 1	2	3	4	5	6	7	8
V = 1					$300	$3K	$30K	$300K
2				$300	$3K	$30K	$300K	$3M
3			$300	$3K	$30K	$300K	$3M	$30M
4		$300	$3K	$30K	$300K	$3M	$30M	$300M
5	$300	$3K	$30K	$300K	$3M	$30M	$300M	
6	$3K	$30K	$300K	$3M	$30M	$300M		
7	$30K	$300K	$3M	$30M	$300M			

If the:

$ Impact of the even is:

$ 10	**V=1**
$ 100	**V=2**
$ 1,000	**V=3**
$ 10,000	**V=4**
$ 100,000	**V=5**
$1,000,000	**V=6**
$10,000,000	**V=7**

Estimated frequency of occurrence is:

Once /	**300 Years:**	**P=1**
Once /	**30 Years:**	**P=2**
Once /	**3 Years:**	**P=3**
Once /	**100 Days:**	**P=4**
Once /	**10 Days:**	**P=5**
1 Time /	**Day:**	**P=6**
10 Times/	**Day:**	**P=7**
100 Times/	**Day:**	**P=8**

Many intersections may describe problems sufficiently small and, therefore, neglected. Ordinarily, if the sum of V and P is less than Six (6), it is reasonable to neglect the intersection. In some cases, it is acceptable to set the threshold higher, but exercise caution. There may be protective measures that will contain a large number of low cost problems but cannot be cost-justified unless you identify these small problems. Take care to avoid disregarding an intersection because only the per-instance dollar impact (V) is low. It may well be that the probability or occurrence (P) is sufficiently high enough to yield a high annual cost (E) for this problem. If, for example the cost of a particular data entry error is only $10, do not ignore it as too small to be important until it is also known that it does not happen many times a day.

There is a strong tendency to attempt to make cost and probability assessments for more exact than are actually required. This contributes materially to the time required to complete a risk assessment, without a corresponding increase in the value of the product. It is common when working with a group engaged in a risk analysis to find the discussion bogged down on the question of whether there is, in a particular instance, an $115,000 or a $130,000 problem, when in fact it makes no difference which value the group assigns.

It is better to do the risk assessment making very gross estimates of both the cost and probability. Refine specific items later only if determined that a decision to pursue a particular solution requires greater precision. For this reason, an we propose an artifice to induce the risk assessment team to be sufficiently “inexact”, at least on the initial pass, to complete the job in a reasonable amount of time. The use of factors of 10 (orders of magnitude) for both dollar cost and probability is recommended.

When performing the risk analysis, be sure to capture and record all three values (V, P, and E) in the matrix. Otherwise, it is sometimes difficult to reconstruct the basis for a particular value of E if the values of V and P are no longer available to reference.

There is also an alternate approach to the matrix. The following description is for those who wish to use a mathematical approach, but you will readily find that the formula yields the same result as the matrix.

Alternate Method:

$$E\ \$\ /\ Yr = \frac{10^{(P + V - 3)}}{3}$$

Where: V = Dollar impact of the event
P = Estimated frequency of occurrence

Probability Analysis

It is important to recognize that assessment of probabilities is dependent on the background, knowledge, and behavioral characteristics of the individuals assigned to perform the risk analysis. This should not seriously inhibit the results.

With on-going systems with which there is a body of knowledge, particularly as it applies to high probability errors and omissions problems, the task of assigning probability is relatively easy. Typically, the team can work from a foundation of experience.

It is usually more difficult to assign probabilities to dishonest behavior problems. Nevertheless, with the proposed gross quantification intervals, it is not impossible. Even if reporting all “white collar crimes” to law enforcement agencies (as opposed to the estimated 10% to 15% of detected Instances), there would still not be a sound statistical base of reliable data to select from. In addition, people are so complex and their behavior patterns so unpredictable, it is utterly impossible to attempt to develop a statistically based behavior analysis relative to the probability of members of groups committing specific crimes. Information judgment based on a thorough knowledge of the environment under consideration is the best approach.

Example:
Common sense is also a very powerful weapon in attacking a probability analysis. In a Life Insurance beneficiary payment system, in which several hundred to a thousand or more people discover that it is relatively easy to change a beneficiary address undetected, there is an exposure to at least one dishonest person successfully diverting checks. Such a situation should yield a probability much higher than once in 30 years, probably much lower than every ten days, and so, using our exponential scale, we may predict either one every 100 days or 3 years. Selection from one of these two choices depends on several factors, including the general climate in which the system functions. If the number of people who know of the potential exposure is in the order of one to two hundred, it is perhaps reasonable to work with a Three Year probability. If the number of such people is in the thousands or if employee dishonesty is a sustained problem, then the One Hundred day approximation is probably better. This selection determined by the risk analysis team. However, the team must consider the general environment. If employee dishonesty is relatively rampant and accepted by management so long as it does not exceed established bounds, then anticipate a much higher probability of loss.

Contingency Planning

Most organizations have a critical dependence on the timely conduct of certain system functions. The functions with critical dependence are usually in the order of 15% to 20% of the total workload. There are notable exceptions but they are relatively few. An important product of the risk assessment is the identification of these time-dependent applications and an awareness of the cost to the organization as a function of the length of time it is without the ability to perform work in this category.

Some of the most important EDP functions, if delayed, will not seriously harm the organization. It may well be that the only economically or technically feasible way of doing these functions is through the use of EDP, but, if the work is delayed a few days, the actual harm or cost to the organization will not be great. Other functions often have heavy dependence for their value on their timely conduct. Online banking operations, retail credit checks, warehouse control, order entry under some circumstances, airline reservations, air traffic control operations and certain command and control operations are examples of functions which are usually quite sensitive to even brief denial of EDP support. Other activities become sensitive only at particular times and these may be relatively infrequent. Stockholder dividend payments, for example, usually occur but four times per year, but it is generally unthinkable that circumstance could delay these checks.

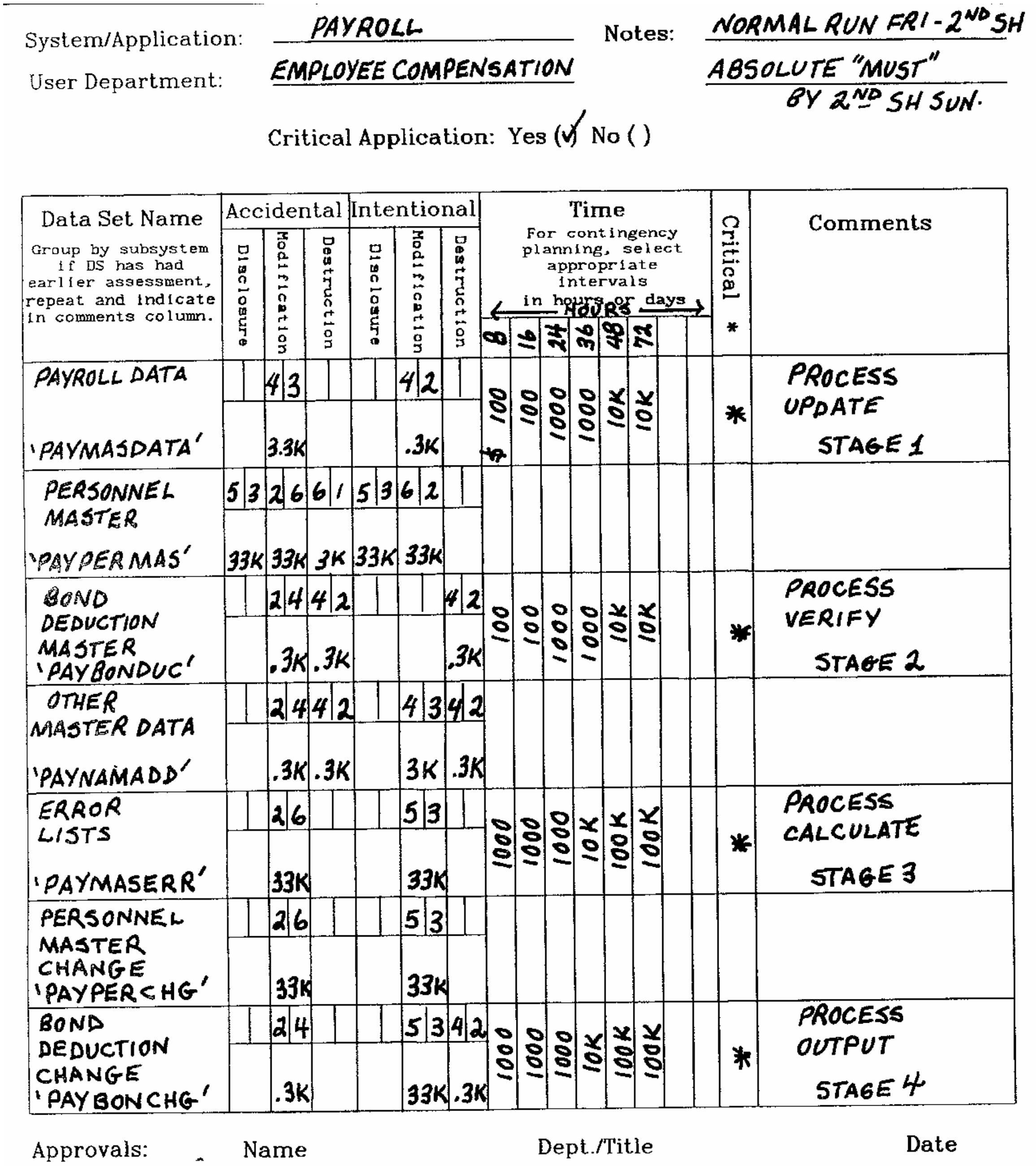
The identification and quantification of any potential problems associated with delaying the performance of critical tasks is usually necessary to the establishment of cost-effective contingency plans. These plans should reflect the needs of the organization for the processing of jobs by the EDP shop. If the nature of this dependence is not known, a good contingency plan is difficult to justify and there is significant risk of spending more, as well as less, than necessary for a workable back-up arrangement.

The need to support contingency planning provides the justification for the time columns on the risk assessment form. The time intervals selected should be appropriate to the particular organization and the particular business function. For example, several commercial banking functions normally have down time costs which will vary rapidly over intervals as short as 2, 4, 6, and 8 hours. On the other hand, intervals of 12, 24, and 36 hours seem appropriate to most life insurance applications. Then again, there are always exceptions that are peculiar to the organization of the business function. Use the comments column to indicate significant periodicity to critical jobs, such as to particular times of the day, days of the week, monthly closings, quarterly dividends, etc. This greatly enhances the value of the risk assessment in support of contingency planning.

It is often stated that there is no justification for an attempt to identify a back-up facility because no one else can possibly spare the machine time necessary to replace the whole capability of the system which is down or which was lost in some fire or other type of catastrophe. The flaw in this rationale is the assumption that it is necessary to find a facility that can replace all of the capability that was lost. It is generally true that only 15% to 20% be specifically identified, and to prepare contingency plans that include the availability of all the things necessary to process elsewhere (including programs, forms, communications, data, and people) in the event of a loss of the primary facility.

Just how many bricks and which ones you can lose before your endanger your foundation, that is for you to decide.

SAMPLE OF FILLED IN RISK FORM



System/Application: PAYROLL

User Department: EMPLOYEE COMPENSATION

Notes: NORMAL RUN FRI-2ND SH
ABSOLUTE "MUST"
BY 2ND SH SUN.

Critical Application: Yes (✓) No ( )

Data Set Name	Accidental			Intentional			Time								Critical *	Comments
Group by subsystem if DS has had earlier assessment, repeat and indicate in comments column.	Disclosure	Modification	Destruction	Disclosure	Modification	Destruction	For contingency planning, select appropriate intervals ← in hours or days → HOURS									
							8	16	24	36	48	72				
PAYROLL DATA 'PAYMASDATA'		4 3 3.3K			4 2 .3K		$ 100	100	1000	1000	10K	10K			*	PROCESS UPDATE STAGE 1
PERSONNEL MASTER 'PAYPERMAS'	5 3 33K	2 6 33K	6 1 3K	5 3 33K	6 2 33K											
BOND DEDUCTION MASTER 'PAYBONDUC'		2 4 .3K	4 2 .3K			4 2 .3K	100	100	1000	1000	10K	10K			*	PROCESS VERIFY STAGE 2
OTHER MASTER DATA 'PAYNAMADD'		2 4 .3K	4 2 .3K		4 3 3K	4 2 .3K										
ERROR LISTS 'PAYMASERR'		2 6 33K			5 3 33K		1000	1000	1000	10K	100K	100K			*	PROCESS CALCULATE STAGE 3
PERSONNEL MASTER CHANGE 'PAYPERCHG'		2 6 33K			5 3 33K											
BOND DEDUCTION CHANGE 'PAYBONCHG'		2 4 .3K			5 3 33K	4 2 .3K	1000	1000	1000	10K	100K	100K			*	PROCESS OUTPUT STAGE 4

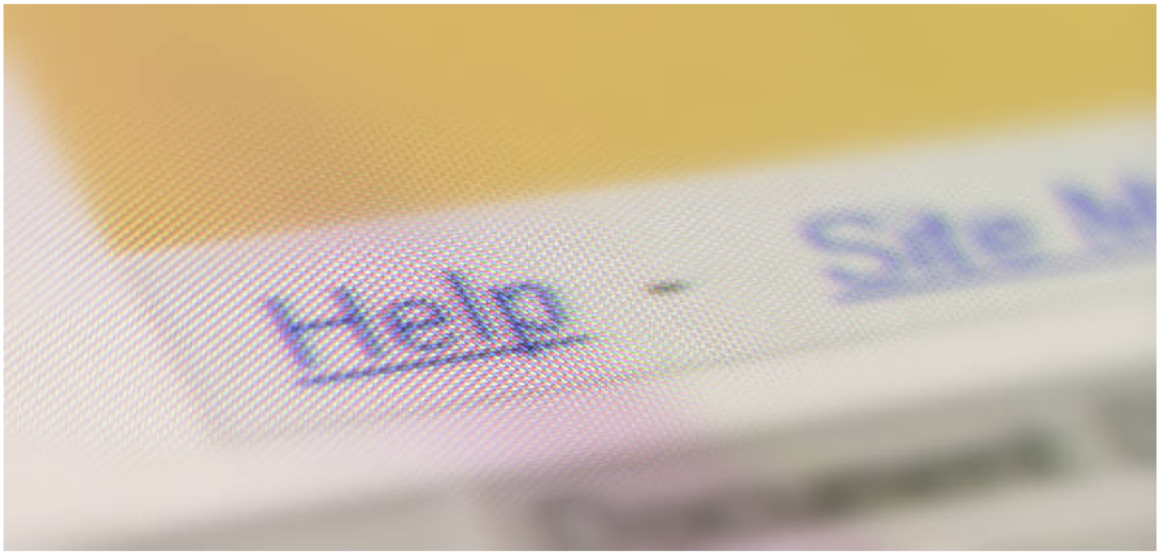
Approvals: Name Dept./Title Date

Helpful Hints

Performing a risk assessment often leads to a number of unanticipated questions in a several areas that may impede progress. The most common areas of concern are:

- Threat Analysis
- Errors and Omissions
- Dishonest Employees
- Personal Integrity
- White Collar Crime
- Physical/Processing Loss
- Fire Damage
- Avoidance of Subdivision
- Security/Risk Maintenance
- Security Assessment Questions

This section of Risk Management provides you with some basic “Helpful Hints” for consideration under each of the most common areas of concern. Your personal knowledge and intuition obtained from your own environment will be an important asset in addressing each of these concerns.



Threat Analysis

Much discussion has taken place on the need to complete a “threat analysis” before a risk assessment can be conducted. The proper scope of that activity is such as to defy so forbidding a title and to make it quite feasibly a part of the risk assessment activity. In fact, it is of some importance that we **‘avoid’** any attempt to list all of the undesirable things that might happen to our data or the means of processing it.

A list of generic threats, such as fire, water, communications failures, power failures, data entry errors, and programming errors is generally adequate. It is far more important to recognize the susceptibility to fire damage of the full array of things on which the EDP facility is dependent than it is to identify all the ways in which a fire can start. Vulnerabilities are far more important to the risk determination than are detailed lists of threats.

Listing threats can be an endless task and experience strongly implies that, no matter how long the list, it will be sufficiently incomplete and planning built about it will be less effective than desirable.

Errors and Omissions

It is important to give **‘proper weight’** to the importance of errors and omissions. It is more likely that people making mistakes will destroy data, render it useless or even harmful than the likelihood of destruction by dishonesty or malice. People whose loyalty and honesty are unquestioned, but who lack sufficient judgment and competence, are the greatest risks. Data security considerations must not be limited to concern for acts of dishonest people. Otherwise, it is very difficult to achieve proper cost justification of appropriate security measures. The principal difference between dishonesty and mistakes lies not in how to thwart them, but in the intent of the offender. They are both costly.

Dishonest Employees

It is of utmost importance when considering the potential for damage by dishonest or malicious people to keep in mind that employees commit the vast majority of all “white collar crimes”, not outsiders.

Most of the losses from dishonest employees occur when employees **‘misuse’** systems resources to which they have authorized access to get their jobs done. The people who steal from Accounts Payable usually work there or have authorization to enter or modify Accounts Payable data. The people who steal from inventory through manipulation of the data processing facility most commonly work in Inventory Control. The people who work in Accounts Payable usually do not steal from inventory or payroll. Keep this in mind when considering the exposures to data security problems. Most of the improprieties related to Data Processing Systems are by the people who work with the particular functional area of the business from which the theft occurs.

Personal Integrity

It is usually best to eliminate **‘perceived’** individual personal integrity when performing a risk analysis. While the probability that an individual will engage in dishonest conduct clearly varies widely from person to person and clearly influences the exposure to problems originating in that manner, the factors that influence individual integrity are not easily perceptible. Further, individual personal integrity is not a constant. It varies dramatically with time and with personal situations of which a risk evaluation team may be completely unaware. Personal pride, frequently reflected in care and precision in the conduct of a job, can also lead to other endeavors to satisfy this pride. Conflicts between two ethics, for example the need to pay for an urgently needed operation on a child and a desire to be honest, can be resolved in a manner not favorable to the employer. The highly motivated employee who feels passed-by on promotions may decide to get his increased income in a manner of his own choosing. For these reasons, it seems most satisfactory to eliminate ‘perceptions’ of specific individual personal integrity as a factor in the risk assessment.

White Collar Crime

A meaningful deterrent to "white collar crime" is to limit its reward to the absolute minimum. If all persons having access to the system have the **'least privilege necessary'** to getting their jobs done, the potential rewards for dishonest conduct are less. Further, most people are strongly deterred by fear of being caught and, to a lesser extent, by fear of formal punishment.

Physical/Processing Loss

The loss of the physical facility itself should be treated **'independent'** from the loss of processing capability. It is misleading to consider the loss of processing capability as part of the cost of the physical facility. The loss of the physical facility, in a properly planned operation, may not result in a loss of all processing ability. The loss of processing ability need not involve the loss of the physical facility. There may be, and, in fact should be, other facilities on which more critical data processing functions can be continued until the prime system is replaced resulting in a cost of loss to the facility only modestly greater than the replacement cost of that which was destroyed. For this reason, treat that loss of the ability to process as a data security problem and taken into account when considering the impact of other problems on specific files.

Fire Damage

When considering the problem of fire, bear in mind that fire can deprive the facility owner of services without destroying or in any way damaging the data processing complex itself. In high-rise buildings, for example, severe fires on any floor below the facility, and, frequently on any floor above, will disable that facility by depriving it of power, air conditioning, communications, and elevators. Fire that destroys the supply of pre-printed paper forms can seriously inconvenience the operations and effectively cripple any function dependent on those forms. It may well take longer to replace a destroyed supply of customized forms than it does to replace the hardware facility. It is necessary to **'consider all aspects'** of each possible loss to fire.

Avoid Subdivision

Whenever possible, it is best to avoid subdividing consideration of the protection of all EDP resources into such categories as 'Data Security' and 'Physical Security'. Aside from such obvious problems as security of data clearly requiring physical security, separating or compartmentalizing concerns **'tends to obscure'** desirable trade-offs between candidate security measures. The problem is often further aggravated by assigning responsibilities to different people. Whether assigned to different people or not, however, the subdivision should be avoided. As an example of the potential for unfortunate consequences if we do take the problem apart, consider the need to identify terminal operators to the system in order to hold them responsible and accountable for their actions. Suppose, also, that we elect one of the better ways of doing that; that is, with magnetic stripe cards. To keep terminal users from giving or lending their cards to each other we should also consider using the same controls and cards for access control to the building and/or work areas.

We have seen several instances where, because of dispersion of responsibility for security among several people, magnetic stripe cards used at the terminals but other, incompatible means used on the doors. Thus, the employees were required to either; carry a variety of cards or carry cards and memorize cipher-lock codes as well. There is an 'attendant' security loss as well because it is now **'difficult to correlate'** who came in the work area with who with who used the terminal.

Another division of concern which is less common than the data and physical one is the occasional **'unwillingness to recognize'** losses resulting from errors as security problems, or, if recognized as such, treating them separately. This too can have unfortunate consequences as it negatively effects the cost justification of security measures by limiting the scope of the problem to which any particular measure is applicable. As another example, some of the most essential security measures, such as personal identification of terminal users, can serve to identify people who are making mistakes as well as people who might have engaged in dishonest behavior. In general, there are so many more people making mistakes than there are actively dishonest people that the potential for dishonest alone might not provide sufficient justification for the needed personal identification mechanism. Combined, errors and dishonesty together might provide more than adequate cost justification for appropriate protective steps.

Security/Risk Maintenance

The output of a successful risk assessment should be a **'quantitative expression'** of potential exposures to the organization; by specific categories of risk – to specific EDP applications – required to support specific critical business functions.

This output should include enough detailed explanation and supporting rationale to be **'easily** understood' by the management decision makers expected to support and fund action based on the data it supplies. The Risk Assessment Project concludes once management accepts and acknowledges it as valid.

A pitfall that many organizations fall into is that of treating risk assessment as a one-time project. This flaw requires serious rethinking on the part of upper management. Data processing support of an organization is not static. It is constantly changing shape and form – almost daily. New applications replace old ones to support new or existing business functions. It is necessary to modify old applications to support new business requirements. **'New risks continue to emerge'** as a result of new applications and/or changes to old applications, and the probability exists that these new risks may be even greater in magnitude than those identified by the initial risk assessment 'project'.

A result of this dynamic environment, created by the increasing dependence of the organization on data processing, risk assessment is an on-going process in the organization. Every new application and/or every major modification to an existing application should have an associated security risk assessment included as a **'primary task'** of the application or change 'project plan'.

In addition, **'periodic** reassessments' of at least the 'key critical applications' which support major business functions should be completed with formal reports to management on the results.

Security Assessment Questions

As stated earlier, the goal of a risk assessment is “the implementation of controls which, costing significantly less than suffering the problems to which they apply, bring the associated EDP operations risk to an acceptable level”. An integral step in any risk assessment project should be an evaluation of existing security measures versus the associated risk potential for the determination of specific actions required to either strengthen and/or relax security controls.

Executive Blueprints provides a comprehensive Security Assessment Questionnaire. You can obtain this material by accessing the training module “Security is a Management Issue” at www.ExecutiveBlueprints.com

This document can be useful to Data Processing management, general management, auditors, and risk assessment teams in evaluating and developing security programs and highlighting those areas that need additional management attention.

This questionnaire requires simple yes/no answers to a series of questions in fourteen categories under three major security areas:

- ✓ **Physical Security:** Fire, Rising Water, Falling Water, Intrusion
- ✓ **Controls and Procedures**: Organizational Controls, Personnel, Operational Controls, Interface Controls, Application Development, Other
- ✓ **Contingency Planning:** General, Emergency, Backup, Recovery

At the end of each category, is an area to summarize your evaluation of the security position pertaining to that category such as:

- ✓ ***Extremely low risk*** *(consider opportunity to relax controls)*
- ✓ ***Necessary risk only*** *(no action indicated)*
- ✓ ***Acceptable*** *risk (this risk is known to and accepted by a level of management with sufficient discretion and resources for all corrective action)*
- ✓ ***High Risk*** *(need for action indicated)*

While this questionnaire is comprehensive, it is not exhaustive. For very sensitive environments, applications, or data, more extensive testing may be required.

The Risk Analysis Team

Team Composition

The composition of the team to perform the risk assessment is particularly critical to its success. **It is not feasible to do the job both quickly and well.** It takes time. With even the best teams and a near optimum situation, experience has shown that the time required is about one month for each 2000 data sets or files under consideration.

The proper consideration of the impact and probabilities required to complete the recommended procedure requires the assignment of well-informed, properly motivated people. **Do not delegate the job as a routine task.** Because it takes good people and, in a large organization, quite a while, it is suggested that the best way to convene a good risk analysis team is to agree that the people working on it will be required for only a half day per day with the other half spent in normal duties. The alternative to this mode of operation, the full-time task force approach, seems to provide only a fast wind-up with a quick fade before a significant amount of work is completed.

The participants on the risk assessment team must include competent, senior representation from each of the following:

- ✓ Information systems operations management
- ✓ The department supported by or owning the data ‘under consideration at this time’
- ✓ The programmer(s) responsible for support of the department, operation or function currently under consideration
- ✓ Systems programming, if the installation is large enough to require such a function
- ✓ The data security coordinator or administrator in EDP, if any exists
- ✓ The communication network administrator, if any exists
- ✓ The data base administrator, if any exists
- ✓ The internal audit function
- ✓ The department responsible for physical security

Management Commitment

Strong senior management commitment to risk assessment is essential to its success. No amount of lower level concern will be truly effective unless everyone who has a role in achieving security believes that the senior management has sufficient commitment to this area. It is often difficult to convince senior management that they should be concerned without a quantitative expression of the problems as might be derived from the risk assessment. This situation leads to a chicken and egg syndrome. There is a need for senior management support to organize a properly manned risk analysis team, but management may not be sufficiently concerned about data protection until they see the product of the assessment for financial risk.

IMPLEMENTATION CHECKLIST

Check these process steps for implementation status

In Place	Process Action	Needs Work
	We have Senior Management support to do a risk assessment	
	We have identified the risk assessment team participants	
	We have identified all of the critical business applications	
	We have identified and involved all critical application owners (*)	
	We have identified custodians and users of critical applications (*)	
	We have agreement on our risk assessment methodology	
	We have tested our methodology for reasonableness	
	We have provided for inclusion of new critical applications	
	We have a notify process when critical applications are modified	
	We are confident that our program will meet our present and future needs	
Of Ten	How Did You Do? Are You Ready to Implement?	Of Ten

(*) Do you need help?

See the "Ownership and Classification" training module, also available from www.ExecutiveBlueprints.com

REVIEW THE RISK MANAGEMENT PROCESS

- ☐ Have we adequately identified our critical information assets

- ☐ Have we analyzed our ability to protect our proprietary information

- ☐ Have we provided for adequate protection

- ☐ Have we considered needs and opportunity to enhance our procedures

- ☐ Have we gained the support of all employees to protect our assets

About the Author:

Louis W Mehrmann
Biography

Summary

“Lou” Mehrmann is a retired free lance Business Management Consultant with over 45 years of customer focused interrelationships and business process experience. He began his business career when he joined IBM immediately after serving in the U.S. Navy during the Korean “Conflict” where he earned his Dolphins aboard the Submarine U.S.S. Sennett (SS408) as an Electronics Technician.

Lou has 35 years of diversified IBM experience; in field, headquarters, line, staff, and management positions; in service, marketing, and corporate business functions. His major strengths are in business process planning/management, process problem/causal analysis, solution design/implementation, and standards. He has specialized knowledge in Information Systems Management, Data Security, Audit Practices and Procedures, and Baldrige Quality Assessments. He is a creative, energetic results oriented professional, whose work ethic, example, and exceptional rapport with younger employees build strong team commitment

After retiring from IBM, Lou spent:

- Two years as a consultant with the IBM Credit Corporation base lining, entitling, and reengineering their field marketing process.
- One year consulting with medical practitioners performing office work flow time/motion studies, evaluating staff assignments, making staffing recommendations, and in the evaluation of overhead expenses and recommended cost reductions.
- Five years as a consultant, again with the IBM Credit Corporation designing, implementing, and managing an end-user Customer Satisfaction Program.
- Two years with DBA Business Transformation Services doing self-study course evaluations and recommendations, learning activity identification to support specific skills, career path roadmap definition and design, and in evaluation of participation by business unit and profession in the career planning process.

About the Author:

Louis W Mehrmann

Accomplishments

Initiated, developed, implemented information systems management briefings, seminars, planning sessions to address customer concerns about complexity, reliability, availability issues resulting in eased transition to new applications, decreased pent up demand and increased productivity. Lou conducted sessions for several hundred customers including more than a dozen Fortune 500 establishments.

Lou designed, developed, and published twelve customer data control documents for IBM. (Security Assessment Questionnaire, Security Controls and Procedures, Risk Assessment, Contingency Planning, Dial-Up Security, Information Ownership and Classification, Personal Computer Security, Control of Off-Site Terminal and Software Usage, Information Systems Network Security, Fire Suppression in DP Operations, Bibliography of Security, Audibility, Control Publications, and a Detailed Three Phase Project Plan for Implementing System Network Control Centers).

Lou counseled over 3000 IBM customers nationwide via seminars relating to security, audibility, and control of information systems to address data integrity and corporate Data Asset Protection issues. This resulted in heightened customer awareness and implementation of improved protection methodologies.

Developed and initiated three new corporate audit programs for IBM; (Personal Property Taxes for M&D Sites, Buy America Procedures and Controls, Import Process Controls) which identified a lack of business process controls over several critical business functions exposing the corporation to significant financial loss opportunities. Resulted in major changes to worldwide sourcing logistics system and strengthening of associated internal controls. Participated in 12 audits, acted in capacity of Auditor in Charge for 11 additional audits, Mentored and trained six new audit team players.

Facilitated documentation and analysis of IBM field technical support process that identified significant redundancies. Resulted in initiation of major process re-engineering project to affect ten times (10X) improvement in process effectiveness and efficiency.

Developed, implemented, and managed an End-User Customer Satisfaction program for IBM Credit Corporation. Established closed loop process to identify and correct systemic root causes of customer dissatisfaction.   This resulted in 8% (87%-95%) improvement in overall customer satisfaction and designation as “Best of Breed” within IBM parent company.

About the Author:

Louis W Mehrmann

<u>Personal</u>

Lou is a prostate cancer survivor, having both surgery and radiation after diagnosed less than one year after retiring from IBM. Since that time, both Lou and his wife Gloria have been actively involved in promoting cancer awareness in a variety of ways. Lou developed and provided the American Cancer Society (ACS) a presentation on prostate cancer that is readily available to deliver to any organization with an interest in the subject.

Lou personally presented to over 100 business, fraternal, university and church organizations in Southwest Virginia. He has been actively involved with the American Cancer Society as a committee Chairman for cancer education and on the local ACS board of directors. Lou is also an active member of the planning committee for the local Man-to-Man prostate cancer support group sponsored by ACS. In recognition of his dedicated service, Lou was selected and participated for several years in the Department of Defense (DoD) Prostate Cancer Research Program as a consumer advocate to evaluate proposals from medical professionals competing for research funding.

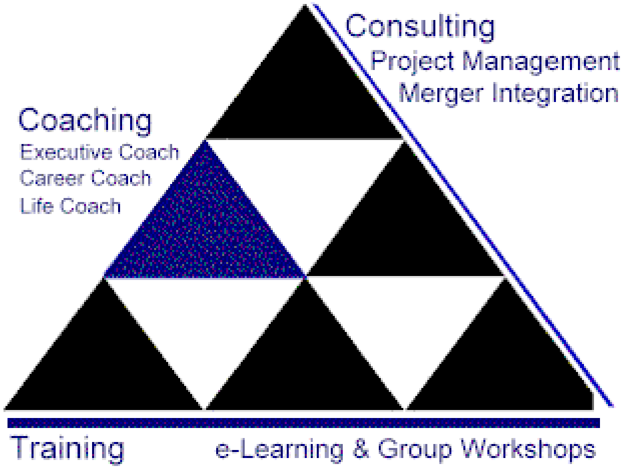
In response to requests, Lou and Gloria established a volunteer program for cancer advocates to support the Southwest Virginia Cancer Center. As a couple, they became active participants in the Man-to-Man program and selected to participate in the American Cancer Society National Cancer Awareness Education Council. They developed several training modules to teach selected leaders how to establish, organize, and run successful Man-to-Man functions for ACS. They personally trained new Man-to-Man leaders in several cities across the mid-south region of ACS.

About WWW.EXECUTIVEBLUEPRINTS.COM

Time is Money

More Impact, Less Interruption

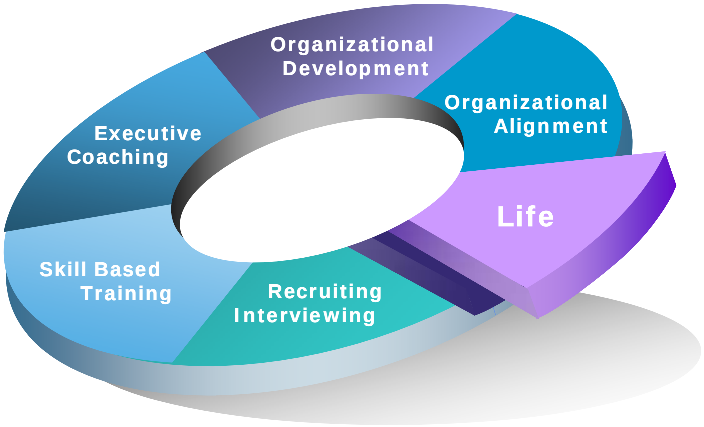
Fast Paced, Results Based Consulting, Training and Coaching



The foundation of every organization is the talent of the people within it.

Executive Blueprints, Inc is dedicated to supporting leadership by providing proven blueprints for success and individual resource development. Services include preparing a customized library of training and reference materials, consulting and management coaching.

Executive Blueprints uses experienced executive talent with customized materials to enhance personnel at all levels of an organization. From Executive Coaching to Management Development, Associate enhancement and New Hire selection techniques, we are dedicated to help measure and achieve success. Let us help you reach your goals with the right tools for continuous self-improvement.



Executive Blueprints, Inc is not engaged in rendering legal or financial advice. These tutorials are not a substitute for the advice of an attorney or accountant. If you require legal advice, you should seek the services of an attorney. If you require financial advice, you should seek the services of an accountant.