Risk Management

James W. Meritt
Jim.Meritt@Wang.com
(703) 827-3534

Abstract

To believe the news media, there are a host of cruel and omnipotent hackers out there who can totally destroy any system they set their minds to, spreading total devastation upon whoever and wherever they wish. The slightest freak of nature - heavy rain, a fire, a date on a calendar - can wipe any system out entirely. This is not the case: the devastation is not total, the destruction is not complete there are countermeasures that can be brought to bear to avoid this disastrous outcome.

Introduction

There are a number of very real risks to information systems, but they are not absolute. There is a chance of any system being subject to attack, but it isn't certain. You are not subject to the whims of the attacker or of nature, there are many things which can be done to mitigate the losses.

Risk management is the total process of identifying, measuring, and minimizing uncertain events affecting resources. This paper was written to help in the objective analysis of the risk management process.

The Office of Management and Budget CIRCULAR NO. A-130 dated February 8, 1996 states: "The Appendix no longer requires the preparation of formal risk analyses. In the past, substantial resources have been expended doing complex analyses of specific risks to systems, with limited tangible benefit in terms of improved security for the systems. Rather than continue to try to precisely measure risk, security efforts are better served by generally assessing risks and taking actions to manage them. While formal risk analyses need not be performed, the need to determine adequate security will require that a risk-based approach be used. This risk assessment approach should include a consideration of the major factors in risk management: the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards." For this reason, many Federal, including Department of Defense, agencies have not performed a formal risk analysis but have instead opted for a less-extensive facilitated risk assessment process. For this reason many of these methods are not required and may not be familiar, but may help in the preparation of a comprehensive risk assessment.

Evaluating What Is At Risk

Every asset has an associated cost. The cost of physical assets should be the at least the replacement cost, which should also include inflation rates. Categories that should be considered are:

> Facilities: All buildings, air conditioning, furnishings and other support equipment. Excludes any asset more properly classifiable in another asset category. Think of things like "fire" or "flood". Other possibilities include earthquake, bombs and chemical contamination, which causes the EPA to close the facility. The cost associated with computing resources can be the cost to run the resource for a given time period, or by estimating the time required to rebuild/compile, test and re-install.
>
> Equipment: All information system equipment located in the contiguous area. Does NOT include equipment that would NOT be lost, say, in a fire that completely destroys the computer facility such as relay equipment under a manhole cover or mounted on a telephone pole outside of the facility. Everything that you had to buy and install in the center- you should be able to get the purchase price real easy. And check the maintenance agreement - there may be some proviso in there amongst the warranty information.

Software: All programs and documentation that would be lost if the computer facility were completely destroyed. This can be broken down into:

Commercial - You bought it, you can consult your receipt. Check the warranty information, because it may be replaced for free in the event of disaster.
Proprietary - You developed it yourself. How much would it cost to re-create it?

Records and Files: All magnetic media data files that would be lost if the facility were completely destroyed. Simply count and multiply. The information content of those items is covered next.

Data and Information: An arbitrary value methodically applied to represent the value of all data and information maintained in the computer facility; including any losses that might occur were the data compromised but not necessarily destroyed.

For estimating the costs of the data itself, talk to the information owners: find out how much time and resources would be required to replace it (if they need to replace it all). Cost time and resources - the procurement department should be able to cost staff time when needed. One measure is the labor needed to recreate it. To this should be added the "opportunity cost" -- the money unearned because one is busy recreating instead of proceeding with other business. Try to estimate impact on the business: ask questions such as: "can you do your work without this data? If not, can the company operate without revenue until you get the information back?" and so on. Estimate cost of this impact (taking into account intangibles such as loss of business, loss of reputation, etc.). Internal/external auditors should be able to help do the cost estimating.

Information results from the processing of data. Although there are ways to quantify and characterize data, measuring the value of information is more difficult. Often a small amount of information will have greater value than large amounts of other information. The need to design cost-effective information protection architectures adds new urgency to this classic problem. There is no one metric that applies to all circumstances, but an approach using multiple metrics, each looking at one aspect can still be useful. Although it would be nice to have a simple way of assigning an absolute value to information, it may be more useful to assess value is relative to some context including the uses that are to be made of it as well as the actions of competitors or enemies.

There are different types and places where information resides in an organization and methods to assess its value in each of these. Vital Information exists in:

- Vision or Mission Statements,
- Strategic Plans or Operational Concepts
- Business Processes
- Corporate Databases
- Information System Resources including the capabilities of the knowledge workers whose expertise makes things function. (These resources are the ones that you will probably be more concerned about.)

The cost associated with intellectual property should take into account how the organization would react if the data were to be totally compromised.

Some types of information, such as trade secrets are valuable because they enable it to build better products or conduct a type of business more ably than those who don't share these secrets. This type of information can lose its value should it become commonly available. The same is true of intellectual capital such as software or copyrighted literature. Regardless of other functional or societal value it may carry, its commercial value derives from its ability to influence purchases or products containing it.

Other types of information such as advertising or political ideas increase in value when they are widely distributed or shared. Their value lies in the impact they have on actions such as purchasing or voting decisions.

Negotiables: The value of all negotiable items produced by the computers operated in the computer facility which might be fraudulently misappropriated, etc. by transactions entered into, created by, or otherwise processed in the computer(s) located in the facility, even though the eventual loss might be directly caused by another computer, another manual operation, or a combination of the two.

Material: The value of all tangible property controlled by or accounted for by the computer(s) operated in the facility which might be fraudulently misappropriated, etc., by transactions entered into, created by, or otherwise processed in the computer(s) located in the facility, even though the eventual loss might be directly caused by another computer, another manual operation, or a combination of the two.

Mission: The value of the operating budget of all activities using the computer facility, factored by the workload of these same activities that could not be performed without the computer. That is the exchange value of all the functions dependent on the computer facility, reduced by the percentage of that dependency.

Personnel: An oft-overlooked resource. Remember that **SOMEONE** takes care of and operates these things! There is an entire IS staff to consider, as well as whoever else has operating responsibilities. Some of these individuals are critical - for example, the person who changes the tapes, whoever performs system administration duties, keeps the network up, keys in the volume of text…. As a very beginning, you will need the salary data and what it would take to hire a replacement if they happened to get hit by a bus. The Human Resources department may be able to help with this information.

Goodwill: "Goodwill" might not sound significant, but in taxation/accounting terms, it can be one of the very largest assets a company has. It also is something that is explicitly sold (or not) with a dollar value when a company is evaluated and/or sold. Some people you are dealing with may reduce their estimate of your company's abilities should they find out that the data was lost or that you had to bother them to get some aspect of the data back.

Other factors which are even harder to estimate, but which need to be taken into account, are:

- Embarrassment to the organization
- Financial impact of the loss of confidentiality of the information
- Legal impact
- Pricing the loss of availability of the information

Actual Threats to the Information Systems

A risk is the loss potential that exists as the result of threat and vulnerability pairs. A number of threats and an evaluation of the areas in which they are threats and a measure of concern that each risk exists are listed. A threat is “any force or phenomenon that could degrade the availability, integrity or confidentiality of an Information Systems resource, system or network. One definition is “any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of use.”

For each threat, an individual needs to estimate the loss if the threat were to occur. Therefore, an individual needs to know:

- the replacement cost
- the cost to recreate intellectual property

- the value of an hour of computing time.
- Other considerations (embarrassment, loss of confidence,…)

Here is one way to classify the type of risk to the resource that a particular threat poses. The classifications are availability, confidentiality and integrity.

- Availability - This is broadly defined as having the resource in a given place, at the given time, and in the form needed by the user.

- Confidentiality - Some define this as "The concept of holding sensitive data in confidence, limited to an appropriate set of individuals or organizations".

- Integrity - One can define this as "The ability of an AIS to perform its intended function in a sound, unimpaired manner."

Some of these threats - though not necessarily all - are given below. Naturally, you must consider your own situation. Some threats will not matter and may be dropped from consideration and there may be unique considerations with your specific site.

Threats: Assets at Risk

Facilities: Environmental risks cover things such as floods, lightening, earthquakes, tornadoes… There should be a local meterological office that could provide information on this, but quite likely a large insurance company should be able to supply more information than you need as part of their policy pricing information. Additionally, consider flooding from such things a firemain leaks, fire extinguisher sprays, fires, contamination, traffic coming through the front of the building or hitting power poles and even bombs - real or even threatened.

Equipment: Power surges can come over the powerlines and damage the equipment, fire extinguishers and plumbing leaks which are VERY bad for electronics, some equipment may be dependent upon air conditioning and some may even "develop legs and walk away"! Additionally, care should be taken that equipment is not used for unauthorized purposes.

Software: Programming can be accidentally (or intentionally) modified or destroyed by programmers or even users. Interrupting the power to an operating system is one method by which the programs that are running may be corrupted. The backup process often has the ability to destroy programs as well as data if improperly used, such as if the "restore" capability is triggered improperly. There is also the risk when installing or upgrading programs that the new code is itself corrupted.

Records and files: How safe is the storage of the media? Could they become lost or damaged? Are they stored in a location where they may be considered "surplus" or "for general use"? If the media is lost or stolen, consider the impact of not only the missing media but also the information on it.

Data and Information: This is where the risk of "crackers and hackers" may manifest themselves. Information is something that can be copied or examined without the owner being any the wiser Information on disk may be copied, read or even erased from remote locations through network connections. The media - external copies, pages of printout, even the computer itself - may be subject to the possibility of damage, loss or theft.

Negotiables and other material: This area includes problems derived from unauthorized transactions being performed on the computer such as:

a) A retail location may find it has "sold" a thousand items and mailed them and have an invalid credit card number

b) Something that was sold in confidence becoming public knowledge
c) Something for which the customer is depending on gets “lost” in a fraudulent manner.

Another risk is if there are online control systems which may be corrupted. These days power, lights, air conditioning and more are likely to be under computer control. Many sites have their internal control records maintained online. The transfer of items from one location inside the organization to another is recorded - or even ordered - through computer. This includes things like service orders. There is a possibility of these orders being corrupted, deleted or even falsified.

Mission: The threats to your organization are limited only by the risks the organization exposes itself to. The more an information system is used, the more vulnerable it becomes. There may be forged email, the legal record may become published in the local newspaper, competitors may find out proprietary information - the list goes on and on and can only be determined by the ones in the know: **YOU**.

Personnel: A brief talk with a local insurance company will reveal a multitude of risks: vital individuals may get hit by cars, an epidemic may run rampant across the secretarial pool or even the competitor may decide to pay more.

Other risks which may be experienced

Fraud and Theft

Information technology is increasingly used to commit fraud and theft. Computer systems are exploited in numerous ways, both by automating traditional methods of fraud and by using new methods. Financial systems are not the only ones subject to fraud. Systems which control access to any resource are targets, such as time and attendance systems, inventory systems, school grading systems, or long-distance telephone systems.

Fraud can be committed by insiders or outsiders. Insiders who are authorized users of a system perpetrate the majority of fraud uncovered on computer systems. Since insiders have both access to and familiarity with the victim computer system, including what resources it controls and where the flaws are, they are in a much better position to perform the fraud and have potentially more to gain. An organization's ex-employees may also pose threats, particularly if their access is not terminated promptly.

Malicious Hackers

Hackers (sometimes called crackers) are a real and present danger to most organizational computer systems linked by networks. From outside the organization, and sometimes even from another continent, hackers have broken into computer systems and compromised the privacy and integrity of data before the unauthorized access is even detected. Although insiders cause more damage than hackers, the hacker problem remains serious and widespread.

Studies by the National Research Council and the National Security Telecommunications Advisory Committee show that hacker activity is not limited to toll telephone fraud. It also includes the ability to break into telecommunications systems (such as switches) resulting in the degradation or disruption of system availability. While unable to reach a conclusion about the degree of threat or risk, these studies underscore the ability of hackers to cause serious damage.

The hacker threat often receives more attention than more common and dangerous threats. The U.S. Department of Justice's Computer Crime Unit suggests three reasons. One, the hacker threat is a more recently encountered threat. Organizations have always had to worry about the actions of their own employees and could use disciplinary measures to reduce that threat. However, these controls are ineffective against outsiders who are not subject to the rules and regulations of the employer. Secondly, hacker attacks make people feel vulnerable because the perpetrators are

unknown. And finally third, organizations do not know the purposes of a hacker; some hackers only browse, while some steal, and yet others cause damage. This inability to identify the hacker's purpose can suggest that hacker attacks have no limitations.

Industrial Espionage

Industrial espionage involves collecting proprietary data from private corporations or government agencies for the benefit of another company or organization. Industrial espionage can be perpetrated either by companies seeking to improve their competitive advantage or by governments seeking to aid their domestic industries. Foreign industrial espionage carried out by a government is known as economic espionage.

Industrial espionage is on the rise. The most damaging types of stolen information include manufacturing and product development information. Other types of information stolen include sales and cost data, client lists, and research and planning information.

The Central Intelligence Agency states that the main objective of industrial espionage is to obtain information related to technology, but that information on U.S. Government policy deliberations concerning foreign affairs and information on commodities, interest rates, and other economic factors is also a target. The Federal Bureau of Investigation concurs that technology-related information is the main target, but also cites corporate proprietary information such as negotiating positions and other contracting data as a major target.

Malicious Code

Malicious code refers to viruses, worms, Trojan horses, logic bombs, and other "uninvited" software. Malicious code is sometimes mistakenly associated only with personal computers, but can also attack more sophisticated systems. Moreover, the actual costs attributed to the presence of malicious code have resulted primarily from system outages and staff time involved in repairing the systems. It should be noted that these costs could be non-trivial.

Examples and explanations:

Virus: A code segment which replicates by attaching copies of itself to existing executables. The new copy of the virus is executed when a user executes the new host program. The virus may include an additional "payload" that is triggered when specific conditions are met.

Trojan Horse: A program that performs a desired task, but also includes extraneous functions.

Worm: A self-replicating program which is self-contained and does not require a host program. The program creates a copy of itself and causes it to execute. No user intervention is required. Worms commonly utilize network services to propagate to themselves other host systems.

Threats to Personal Privacy

The accumulation of vast amounts of electronic information about individuals by the government, credit bureaus, and private companies combined with the ability of computers to monitor, process, aggregate, and record information about individuals have created a very real threat to individual privacy. The possibility that all of this information and technology could be linked together has loomed as a specter of the modern information age. This phenomenon is known as "big brother."

The threat to personal privacy arises from many sources. Several cases have been reported involving the sale of personal information by federal and state employees to private investigators or other "information brokers." In 1992 the Justice Department announced the arrest of over two dozen individuals engaged in buying and selling information from Social Security Administration (SSA)

computer files. In the course of the investigation, auditors learned that SSA employees had unrestricted access to over 130 million employment records. An investigation into one region of the Internal Revenue Service found that five percent of the employees had browsed through tax records of friends, relatives, and celebrities.

As more of these cases are exposed, many individuals express increased concern about threats to their personal privacy. Over the years, Congress has enacted legislation, such as the Privacy Act of 1974 and the Computer Matching and Privacy Protection Act of 1988, which defines the boundaries of the legitimate uses of personal information collected by the government.

The President's Commission on Critical Infrastructure Protection identified a wide spectrum of threats, most of which I have already covered:

- National Events and Accidents
- Blunders, Errors, and Omissions
- Insiders
- Recreational Hackers
- Criminal Activity
- Industrial Espionage
- Terrorism
- National Intelligence
- Information Warfare

Numeric and Objective Risk Analysis

Human beings are phenomenally poor at estimated the probability of a risk. Estimation problems often arise from assigning a higher likelihood to what they see or to their perceived the significance. To help correct for this problem, an adjustment may be made by forming three separate "guesstimates": the minimum chance of something occurring, the most likely chance, and the greatest likelihood. The minimum is added to the maximum and the total added to four times the most likely value. The resulting sum is then divided by six. This process is used to derive the average value, instead of what would be the most likely value.

Some chances of events occurring may be gathered from What are the Chances by B. Siskin and J. Staller.

- Chances of being struck by lightning in your lifetime: 1 in 600,000
- Average American is 99.8% likely to live at least one more year
- The chance a devastating earthquake will hit southern California in the next 25 years:50%

The **C**omputer **E**mergency **R**esponse **T**eam Coordination Center cataloged 2,134 computer security incidents reported in 1997, along with 311 vulnerabilities.

Instead of performing all of the estimations and calculations, it may be possible to consult historic data for similar systems and get a usable ballpark value for the annual loss expected based upon their systems (after necessary corrections). Whenever possible, get historic information on a particular threat likelihood. Insurance companies make their living from compiling just these statistics.

After identifying the threats and risks to the system, the following is a method to quantify the impact of the potential threats to the system. For each threat, the probability of that threat occurring and the damage that would result if it were to occur must be considered. Countermeasures to these risks must be identified to mitigate these risks and priced accordingly. In this way, a balance may be reached between "cost" and "risks" so that management can decide which risks to prevent, limit or accept

Each threat must be assigned an Annual Frequency Rate (AFR). The AFR is the estimated number of times a given threat is likely to occur in one year.

For ease of calculation and estimation, fit the estimates into “bucket holes” of rounded-off values of factors of ten, as follows:

- once in 300 years (.003)
- once in 30 years (.03)
- once in 3 years (.3)
- once a year (1)
- once in 100 days (3)
- once in 10 days (30)
- once per day (300)
- 10 times or 100 times per day (3000)

When making your estimates, remember the tendency of people to form their estimates around modes (most common) instead of means (most likely) and take that into consideration in your calculations. As noted earlier, one method is to add the minimum cost estimate to the maximum cost estimate and add the sum to four times the “most common seen” estimate then divide the resultant by six.

The next phase is to assign an Annual Loss Expectancy (ALE) to each threat. This is how much can be expected to be loss in an average year. It may be calculated by multiplying each loss times the frequency of its occurrence.

- For accidental human threats, such as operational errors or system programming errors, the ALE will be a measure of computer down time.

- For natural environmental threats, such as floods or severe storms, the ALE will be based on how much damage and downtime might occur.

- For fabricated environmental threats, such as computer hardware failure, the ALE will be based on the estimated cost to run the system for the time it was down.

How to Mitigate Risk to an Information System

Risks can never be entirely removed. The trick, then is not trying to remove all risks, but to manage them. The secret of effective risk management is the ability to qualify and quantify risk elements objectively and reduce them to acceptable levels. Hopefully the first two parts of this series have helped you do exactly that: identify, qualify and quantify the specific risks to your assets.

A critical aspect of information resource protection to be considered is the need for ongoing management monitoring and review. To be effective, a security program must be a continuous effort. Ideally, ongoing processes should be adapted to include information protection checkpoints and reviews. Information resource protection should also be a key consideration in all major computer system initiatives.

An effective information resource protection program identifies the information used by the agency and assigns primary responsibility for information protection to the managers of the respective functional areas supported by the data. These managers know the importance of the data to the organization and are able to quantify the economic consequences of undesirable happenings. They are also able to detect deficiencies in data and know definitively who must have access to the data supporting their operations.

First, consider each one of the threats faced and come up with a method of managing it. Here are, once again, the major categories of assets that were first introduced in Part 1 and some methods by which

various risks to these assets are handled. It will be up to you to check your personal threats and come up with methods to manage them. The following are items to feed into your own brainstorming session.

Facilities: Insurance companies face this all the time. Off-site warehousing may be indicated. Protection of the site to PREVENT damage may include such things as lightning protection, uninterruptable power supplies (UPS), standby air conditioning, earthquake shock absorbers set in the foundation, fire suppression equipment, roving patrols, and generous amounts of insurance.

Equipment: To protect against power problems, things like an UPS for vital equipment and surge protectors may be necessary. Other equipment protection consists of emergency ventilation in the form of fans, hot spares, standby servers, quick-reaction repair crews, spare parts, covers and/or shields to put over the equipment in case the water sprinklers are activated or a small fire or smoke fills the space, fire extinguisher canisters and flashlights.

Software: Here my emphasis is on backups, backups or maybe backups

Commercial: Keep the original tapes/CDs/other media in a safe place (off site?), spare copies in the facility, have replacement/maintenance as part of the coverage.
Proprietary: Keep spare copies in the facility, additional source code on the system/on hot spares, backups maintained in safe (off-site?) places.

Records and Files (Media): Fireproof cabinets, safe storage (off site?).

Data and Information: Backups, backups and perhaps more backups! This is where the fancy stuff concerning firewalls and proxies come in. Be sure to check what is offered and at what price before you buy, and make sure you can maintain the system! Remember that the hard copy can vanish, be copied, burn,…. .

Negotiables and Material: If the computerized systems don't work, make sure that the "old fashion" one using paper and telephones does! Are ledgers available? Pencils?

Personnel: Can every vital person be reached 24 hours a day? Can he or she get to where their talents and/or skills are needed? Can replacements be found? Are standbys identified?

How to Minimize the Catastrophe

There are a variety of different angles from which this problem could be attacked. In each case, and each angle, you will need an in-depth understanding of such things as the threat, the exposure, the probabilities, the value of the resource, the cost of the protection,…

1. Reduce the Exposed Resource. This may involve removing access to the resource. Methods here involve things such as keeping records in a different location and not putting sensitive information on the computer hard disk.
2. Reduce the Probability of the Threat Occurring. This may involve anything from using more reliable components, moving to a safer location, reinforcing the facility infrastructure, installing multiple redundancies or installing a firewall

In any case, a full understanding of the risk itself is needed, as well as what to do about the individual risk, in order to minimize it.

Risk Acceptance Criteria

After attempting to come up with an appropriate methodology/mechanism to ameliorate the threat, it must be realized that not all risks can be completely overcome. There are individual risky items which cannot be completely mitigated. For each threat, there must be an evaluation made of the conditions under which a risk will be accepted. Two different methods of making this evaluation are given below.

1. Cost/Benefit Considerations

In general, one should never spend more protecting a resource from a threat than it would take to recover from that threat under a worst-case scenario. A cost/benefit analysis should be done to determine if this is not cost-effective. For this analysis to be properly conducted, it will be necessary to determine the costs of the worst-case scenario recovery and the cost of the protection methodology. Note that it may require a bit of brainstorming to come up with the "worst-case scenario". Be sure to include the scenarios which involve not having that resource at all and the re-creation "from scratch" of the resource in your considerations.

Finally, compare the annual cost of the protection methodology with the Annual Loss Expectancies. The acceptance criteria would designate the point at which the cost of the protection methodology/mechanism exceeded the recovery cost of the system which would be protected. Naturally, any no-cost action should be performed. In this case, the acceptance criteria would be that point at which the cost of the protection methodology/mechanism exceeds the benefit of the system.

2. Living with the Possible Consequences

Finally, there are times that you simply have to live with risks and go on. Please note that this is risk dependent and not cost dependent. Sometimes this method will have to be used when even vague cost estimates cannot be made.

For this analysis to be properly conducted, it will be necessary to determine the benefit of the continued operation of the system and the probability that the threat will be realized. In this case, the acceptance criteria would be a subjective evaluation based upon the benefit of the continued operation of the system versus the informed evaluation of the possibility of the worst-case scenario occurring. Before this is accomplished, areas other than financial must be considered. The loss of the confidence of the clients as well as the potential embarrassment of the organization should also be considered.

Keep Track of What is Going On!

A critical aspect of information resource protection to be considered is the need for ongoing management monitoring and review. To be effective, a security program must be a continuous effort. Ideally, ongoing processes should be adapted to include information protection checkpoints and reviews. Information resource protection should also be a key consideration in all major computer system initiatives.

An effective information resource protection program identifies the information used by the agency and assigns primary responsibility for information protection to the managers of the respective functional areas supported by the data. These managers know the importance of the data to the organization and are able to quantify the economic consequences of undesirable happenings. They are also able to detect deficiencies in data and know definitively who must have access to the data supporting their operations

Conclusion

The area of Information Security is not one which contains impossible, unavoidable disasters against which the IS Manager is helpless. The key is to identify, measure, and minimize uncertain events affecting identified resources. This will take individual work, but is doable.

Risk Management

James W. Meritt

Jim.Meritt@Wang.com

(703) 827-3534

Abstract

To believe the news media, there are a host of cruel and omnipotent hackers out there who can totally destroy any system they set their minds to, spreading total devastation upon whoever and wherever they wish. The slightest freak of nature - heavy rain, a fire, a date on a calendar - can wipe any system out entirely.

This is not the case: the devastation is not total, the destruction is not complete there are countermeasures which can be brought to bear to avoid this disastrous outcome.

Office of Management and Budget A-130

The Appendix no longer requires the preparation of formal risk analyses. In the past, substantial resources have been expended doing complex analyses of specific risks to systems, with limited tangible benefit in terms of improved security for the systems. Rather than continue to try to precisely measure risk, security efforts are better served by generally assessing risks and taking actions to manage them. While formal risk analyses need not be performed, the need to determine adequate security will require that a risk-based approach be used. This risk assessment approach should include a consideration of the major factors in risk management: the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards

Evaluating What is at Risk

- Facilities
- Equipment
- Software
- Records and Files
- Data and Information
- Negotiables
- Material
- Mission-related
- Personnel
- Goodwill
- more (embarassment, financial/legal impact, loss of availability,...

Need to know:

- The replacement cost
- The cost to recreate intellectual property
- The value of an hour of computing time
- Other (embarrassment, loss of confidence,…)

Classification of Type of Risk

- Availability
- Confidentiality
- Integrity

Threats: Assets At Risk

By Asset:

- Facilities
- Equipment
- Software
- Records and files
- Data and Information
- Negotiables and other material
- Mission
- Personnel

Other Risks Experienced

- Fraud and Theft
- Malicious Hackers
- Industrial Espionage
- Malicious Code
- Threats to Personal Privacy

The President's Commission on Critical Infrastructure Protection

- National Events and Accidents
- Blunders, Errors, and Omissions
- Insiders
- Recreational Hackers
- Criminal Activity
- Industrial Espionage
- Terrorism
- National Intelligence
- Information Warfare

WANG GLOBAL

Estimating Annual Frequency Rate

- Once in 300 years (.003)
- Once in 30 years (.03)
- Once in 3 years (.3)
- Once a year (1)
- Once in 100 days (3)
- Once in 10 days (30)
- Once per day (300)
- 10 times or 100 times per day (3000)

Annual Loss Expectancy

- For accidental human threats, such as operational errors or system programming errors, the ALE will be a measure of computer down time.

- For natural environmental threats, such as floods or severe storms, the ALE will be based on how much damage and down-time might occur.

- For fabricated environmental threats, such as computer hardware failure, the ALE will be based on the estimated cost to run the system for the time it was down.

Mitigate Risk
to an Information System

Risks can never be entirely removed. The trick, then is not trying to remove all risks, but to manage them. The secret of effective risk management is the ability to qualify and quantify risk elements objectively and reduce them to acceptable levels.

How to Minimize the Catastrophe

- Reduce the Exposed Resource. This may involve removing access to the resource. Methods here involve things such as keeping records in a different location and not putting sensitive information on the computer hard disk.

- Reduce the Probability of the Threat Occurring. This may involve anything from using more reliable components, moving to a safer location, reinforcing the facility infrastructure, installing multiple redundancies or installing a firewall

Risk Acceptance Criteria

- **Cost/Benefit Considerations**

In general, one should never spend more protecting a resource from a threat than it would take to recover from that threat under a worst-case scenario.

- **Living with the Possible Consequences**

Finally, there are times that you simply have to live with risks and go on. Please note that this is risk dependent and not cost dependent. Sometimes this method will have to be used when even vague cost estimates cannot be made.

Conclusion

The area of Information Security is not one which contains impossible, unavoidable disasters against which the IS Manager is helpless. The key is to identify, measure, and minimize uncertain events affecting identified resources. This will take individual work, but it can be done.