Global Information Assurance Certification Paper

Risk Management: A Foundation for Information Security

By: David Litzau

Submitted for GSEC Practical Assignment, version 1.2e on June 3, 2001.

There once was a time not so long ago when a computer occupied an entire building. It was believed that the United States would only need 5 such computers and computer security amounted to making sure that the guard showed up and the door was locked. Today, that same amount of computational power can be carried on your wrist, or in the form of a free calculator from a trade show. But it wasn't the size of the computer that changed information security forever…it was the day that one computer "talked" to another.

Since the mid 1960's, networking, time sharing, multiprogramming, and the Internet have handed out some punishing lessons to those that pushed the envelope to move data farther and faster then ever before. One of those lessons has been the identification of the elements that most need to be addressed when processing data. Those elements are availability, integrity, and confidentiality. If anything threatens these elements, then risk is incurred. It is how to manage that risk that this paper addresses.

Risk Management is a process whereby the assets of a company are identified and assigned a value, probable threats to those assets are identified, and then countermeasures are selected to protect against those threats. Each of these steps are fraught with oversights and often a limited amount of resources to be allocated to the cause. This being the case, Risk Management is often relegated to the back burner.

Identifying Assets

The first step in the process is to determine what you have that's at risk. The short answer is "everything." In order to proceed in some logical order, assets are first categorized into the following groups and are presented here from the most expendable to the most valuable.

Hardware: At first it might be difficult to understand how hardware could be classified as the most expendable asset a company has. The argument could be made that no data processing could take place without it, but hardware is easily replaced and has a known dollar value. With an inventory sheet, a catalog, and a corporate line of credit, delivery of replacement hardware can be accomplished within days.

Software: Software is the component of data processing that manipulates data to suit the needs of its owner. Without software, the above-mentioned hardware amounts to nothing more than appliances. In the case of COTS (Commercial Off The Shelf) software, it is not so much the cost of ordering more software—which would put it in the same category as hardware—but the impact on production if it became unavailable. If the software is proprietary, the value is compounded by the cost of development, testing, and maintenance.

Data: Regardless of how and where data is collected, the collection process itself is expensive. Further, getting the collected data into a data processing system, whether it is keyed in by hand, barcode readers, or scanned, the input process can be slow and expensive. Add these costs to

paying someone to orchestrate the hardware and software to arrange, store, retrieve, and manipulate data, and one begins to see why data takes its place here in the hierarchy.

Policies and Procedures: No business comes with an instruction book on how to stay viable and competitive. Sometimes the margin of success is so thin that a single misstep can spell doom and the doors close. The company has to function in a relatively smooth and predictable manner and this can only be accomplished when everybody understands how, why, and when to perform their assigned duties. This is best conveyed through policies and procedures. These often come at a high price and are learned along the way through trial and error. Learning the best method of doing things sets procedures, and policies are developed to keep from falling victim to previous mistakes. Policies also aid in getting the desired behavior from the employees. Adherence keeps the edge over competition and the company solvent.

People: People are the lifeblood of any organization and clearly the most valued asset a company can claim. The above mentioned assets quickly lose value if not utilized by quality, trained personnel. A business is a collection of people that, as a group, perform a function that cannot be carried out by any one individual.

Classification of assets aids in the Risk Management process by segregating assets into manageable groups. The benefit of grouping assets will become clearer as we proceed through the process.

Getting Started

Serious consideration should be given to forming a Risk Management Team at this point. The team might consist of representation from accounting, human resources, security, and the Department Heads. Their purpose is to begin to place a value, usually in dollars, on the assets previously identified. Department heads make an excellent resource at this stage because of their experience with management of budgets and the unique costs incurred by normal operations.

The most time consuming and labor intensive component of Risk Management is the identification of assets and the subsequent assignment of value. Depending on the size of the organization, the actual inventorying of physical assets can often be carried out as an "all hands" procedure, for larger companies the task of inventorying can be passed directly to mid-management. For this phase an inventory work sheet should be developed. These can be distributed to each employee with instructions to list all the hardware that they utilize. This should include make/model and serial numbers. This data can be used for later development of a hardware inventory database. For now though, this data is relayed to mid-management. . It should be noted that this process likely would not include capitol expenditure items (such as furniture). The focus is to address risk involving data processing operations.

Mid-management becomes the first key player in this phase. With the collected hardware inventory sheets, end users can now proceed with their normal duties.

To make the sheer numbers of raw data that will begin to accumulate more meaningful, a second and more condensed work sheet will be used by mid-management. This sheet will take on a shopping list appearance and will include an itemized list of *hardware, software, data,*

policy/procedures, and *people*. A copy should be maintained for later development of a contingency plan as part of Business Continuity Planning.

Asset Valuation

It is this author's contention that in order to assess accurately the value of assets, weight has to be given to what is known as the *criticality*. Criticality is consideration for the impact that the loss of the asset will have on operations. An asset's value can be greatly magnified by its criticality. For example: The marketing department may consist of 15 Silicon Graphics workstations worth well into the six figures, but each user relies heavily on a shared $100 flatbed scanner. Since the scanner has moving parts and light bulbs, they are prone to failure. Each time a scanner fails, the company is paying the salaries of users sitting in front of thousands of dollars of data processing equipment to do nothing! The $100 scanner can bring the department to a stand still and therefore its criticality greatly exaggerates its cost off the shelf.

One method of including the weight of criticality to the asset valuation process is to assign a weight factor to each asset. By including a section on each asset sheet whereby the risk management team can evaluate the factor based on the following:

- Impact of loss of *availability*
- Impact of loss of *confidentiality*
- Impact of loss of *integrity*
- Impact of *total loss*

Impact of loss to availability and total loss would best fit hardware, but all of the less tangible assets such as software, procedures, and data could be weighted for their impact of loss of confidentiality and integrity. If a scalar value between 1 and 10 were applied to each of the above for every asset, this combined value could be used to assign priority regardless of its dollar value. Policy could be set such that any asset with a combined factor greater than 25 will be addressed in the Threat Analysis phase. This will become very important later when decisions are being made on how the budget is allocated to protect assets.

The actual process of assigning the dollar value to an asset in this process can be a complicated matter that could be addressed by applying a wide variety of accounting theories and various disciplines of mathematics. The key is setting guidelines so that they can be applied universally throughout this phase.

According to Fites and Kratz:

> It is important to avoid "paralysis by analysis" while still doing a thorough job of asset identification and valuation. Too much detail is as bad as too little:
>
> - It is hard to value the "small stuff."
> - The cost of the risk analysis rises.
> - The result can be an overwhelming sea of numbers. (69)

Keeping the assignment of dollar values consistent and straightforward will help avoid the pitfalls mentioned in the quote above. The data collected at this point should be moved to a spreadsheet or database to aid in the next phase.

Threat and vulnerability assessment
At this point, what you have is an accurate assessment of the corporate assets. The collection of such data, if maintained, is an asset in itself and should be protected. So how do we ensure that no harm comes to these assets? In order to respond to this question one must know that which is considered a threat, the probability of that threat occurring, and what impact it will have on the asset.

Earlier it was discussed that grouping assets (hardware, software, etc.) would benefit the process throughout. This is where it begins to assist the Risk Management team. Although some threats can impact all of the groups, there are specific threats unique to each group that will make identifying threats much easier when researching.

Individuals that work with and manage data processing on a daily basis will be able to provide a substantial list of known threats as a result of personal experience. For example:

Hardware: employee abuse, insufficient capacity, mis-configured devices, lost or stolen equipment.
Software: bugs, viruses, backdoors, logic-bombs, upgrade problems, licensing problems.
Data: corruption, loss due to theft, accidental disclosure, storage and back-up problems.
Policies and procedures: poorly enforced, non-existent, accidental disclosure, inaccessible to employees.
People: accidental injuries, poor morale, illness, attrition.

This is in no way an exhaustive list, which emphasizes the next point. The list above may have come to mind from events that have taken place in the past. Any action taken based on this list would be purely reactionary. The Risk Management Team would be derelict in their responsibility if this were the extent of the threat identification. In order to properly assess risk, every effort to identify potential threats must be undertaken. This is where the team will take on the research role. Consider the following resources at this phase of the analysis:

Insurance Companies: Sometimes there is substantial data made available that can assist in identifying threats.

News agencies: Often news articles are archived and available for research. This can be helpful since the data is in searchable databases and can be queried by events.

Local, State, and Federal Law Enforcement Agencies: F.B.I. and other law enforcement statistics and data can assist in the identification, frequency of occurrence, and the impact of illegal activities.

Internet and on-line resources: NEXUS and other companies provide access to extensive databases and indexed archives.

Computer Incident Monitoring Organizations: The SANS Institute, CERT, and others routinely provide notification and archiving of computer incidents such as exploits, viruses, etc.

Research at these sources will provide an excellent starting point. Identified threats should be carefully associated to the appropriate assets. This will bring you to the next phase of the process.

Threat probability and impact

A distinction should be made between *probability* and *possibility*. Is it possible that the company might suffer a meteor strike? Yes…it's possible, is it probable? Not likely. We know this from having researched and not finding any previous occurrences of such an event. We come the point where we must identify those threats that have been uncovered through research, consider the probability of the event taking place, then evaluating the potential impact on the business. This is the point were we will begin to merge data from our Threat and Vulnerability Assessment and the data from the Asset Valuation worksheets.

The frequency of some threats may be difficult to ascertain without historical data. The probability is usually measured in how many times the threat is likely to occur within a year. This fits nicely into the process since the cost incurred in protecting against the threat will eventually become part of an annual budget. The rate of occurrence can be expressed as a fraction of a year as well, where an event has an expected occurrence of once every ten years, the annual occurrence would be 0.1. This is known as the Annualized Rate of Occurrence (ARO).

By first identifying which aspect of the asset will be impacted by the threat (i.e. does the threat compromise *Integrity*, *Confidentiality*, or *Availability*), you can then use the assigned weighted criticality factor as a mathematical component against the dollar value assigned to the asset. The result is a dollar value representing the fiscal impact of the event occurring. This technique may seem like an oversimplification; there are a wealth of theories, methodologies, and high dollar software packages that incorporate a wide variety of statistical and analytical mathematic processes. Regardless of the method used, this value is known as the Single Loss Expectancy (SLE).

By applying the following formula, it is possible to get a dollar representation of what impact each threat is expected to have on the organization. This is known as the Annual Loss Expectancy (ALE).

ARO x SLE = ALE

What have we derived at this point? This value represents the fiscal "Risk" that the organization faces. This value has been adjusted for it's initial worth to the company, the likelihood of a threat occurring, and the weighted impact of the event in a dollar value. Following is suggestions on how to deal with that risk.

Risk Assessment and Countermeasures.

Two key points should be made at this juncture. First; ***there is no budget big enough to eliminate risk!*** The subject of this paper is "Risk Management," not "Risk Elimination." Regardless of the resources allocated toward the defense of an asset, somewhere within lies a flaw or exploit; therefore absolute security does not exist. Second, there comes a point when the

cost of protecting an asset can exceed the value of the asset. A diminishing return on investment means that at some point the cost and the value shall meet.

As the data collected is evaluated, upper management will have to determine what is acceptable risk and how to deal with it. There are four choices that can be made to address risk.

I. Decide that the risk is too high, and there may not be good countermeasures available to mitigate the risk, therefore…eliminate the asset.
II. Decide that there are substantial measures that can be taken to protect the asset and mitigate the risk by doing so.
III. Accept the risk as a cost of doing business and do nothing about it.
IV. Transfer the risk by insuring the asset.

Decisions on the most effective method to select to protect assets should be based on a consensus reached by the Risk Management team with input from the affected parties. Sound knowledge of available countermeasures is crucial at this stage. Often times an effective countermeasure may have little or no additional cost incurred. Once the decisions are made and defenses are implemented, the final phase of the process is reached.

Monitoring of Controls

At this stage, Risk Management moves from a process to an ongoing program. As controls are put into place, the task then becomes providing feedback on effectiveness. If the control is not having the desired result, changes will have to be made. As new threats are identified, new risk is incurred and this information will feed back into the loop so that it can be mitigated. If new assets are introduced then appropriate adjustments will be required, and this sometimes changes how other assets are addressed. Further, if there is a failure to adjust the value of assets as they depreciate or other economic trends affect the value of an asset, then the data becomes invalid.

Benefits of a Risk Management Program

Many aspects of Information Security can utilize the data collected in this process. Besides the obvious gain of implementing safeguards and countermeasures to protect assets, some additional benefits include:

- Asset Identification data can be used for drafting a contingency plan as part of Business Continuity Planning
- Asset Identification data can be used for maintaining a hardware inventory log, often necessary for acquiring property insurance.
- Development of a Security Awareness Training program to teach employees how and why controls are implemented.
- Quick assessment of the impact on the business before implementing new technologies.
- Aids in the development of Policies and Procedures.
- Fiscal impact can be used to get upper management to see the value of an increased Information Security budget.
- Not having a Risk Management Program means that when an asset is threatened, all actions taken are "reactions."
- And more…

Information Security is not the sexiest subject discussed--if ever--in the boardroom of most corporations. Convincing corporate executives to budget money for something that might happen is a difficult proposition. By executing a Risk Management Program, a company has provided a mechanism to illustrate the risk of doing business in dollars, and the impact on the bottom-line is what gains the attention of the executives. As a final thought, we live in a litigious society and our data processing systems are under siege from many fronts. A well-executed program will show the world that "due diligence" has been exercised if ever called upon to do so in a court of law.

Works Cited

Paul, Brooks. "Risk Assessment Strategies." 30 October 2000. URL:

www.networkcomputing.com/1121/1121f3.html (May 24, 2001).

McCarthy, Jim. "MS Solutions Framework: Risk Management." 12 January 2000. URL:

http://www.microsoft.com/technet/Analpln/risk.asp (May 24, 2001).

Australia, Commonwealth of. "Australian Communications-Electronics Security Instruction 33 (ACSI 33)." 30 October 2000. URL:

http://www.dsd.gov.au/infosec/acsi33/HB3.html (May 24, 2001).

Tipton, Harold F. and Micki Krause. Information Security Management: Handbook 4th Edition. Boca Raton: Auerbach, 1999.

Fites, Philip and Martin P.J. Kratz. Information Systems Security: A practitioner's Reference. New York: International Thomson Computer Press, 1996.