Global Information Assurance Certification Paper

Risk Assessment: The Basics

Paul Berryman

February 16, 2002

Introduction

We have all heard the definition of Risk Assessment. In a nutshell, you identify the threats, vulnerabilities, and risks to the system, and then quantify the impact of the potential vulnerabilities. For each vulnerability, the probability of it occurring and the damage that would result if it were to occur must be considered. Countermeasures to mitigate these risks must be identified and their cost determined. A balance must be reached between the cost to mitigate the risk and the cost if the vulnerability is exploited so that management can decide which risks to prevent, limit, or accept.

It sounded so simple the first time I read it. But if you have ever taken on such a project you know it is anything but simple. The first step in assessing the risk in an organization should be to develop a risk assessment process. In this paper I will provide you with a basis for developing this process within your organization. One thing to keep in mind is that risk assessment is an ongoing process. As your business changes, you must reevaluate the security deployed on a system. Also you must ensure the security department is actively involved in system development, including new systems as well as modifications to existing systems, to ensure the appropriate level of security is in place. Not all the steps outlined here may apply to your organization, or there may be some additional areas you may be required to review such as the risk associated with the facilities, software licenses, etc . . . For the purpose of this paper, we will limit this process to the data that resides on the systems.

What are you trying to protect

Before you begin to check your systems for vulnerabilities and mitigate the risks, you must determine what exactly you are trying to protect. For the purpose of this paper we will limit this to the data that resides on the systems.

A complete system inventory must be performed. This may or may not already be available in your organization. A good starting point for determining this may be from your company's disaster recovery or business continuity plan. Also you may want to dust off any Year 2000 documents that may still be available. They may be a little out dated, but could get you started.

I suggest developing a worksheet that will assist you in documenting each of the systems in your organization. Along with documenting the various aspects of the systems be sure to identify all the data and classify it appropriately.

You should also scan your internal network to determine if there are any other systems that may not have been accounted for. Also an external scan of your organizations IP address space will help you determine which systems are directly connected to the Internet, this obviously presents an immediate risk.

Determining Value

James W. Meritt stated, 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?" Estimate cost of this impact (taking into account intangibles such as loss of business, loss of reputation, etc.).

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

Threats to Data

Threats to data come from many different sources, we will focus on four of the more prominent ones, Insiders, Hackers/Crackers, Industrial Espionage, malicious code:

Insiders pose the greatest threat to your data because they have special knowledge of your environment, and they have some or complete access to your systems already. They have established trust relationships with individuals who might otherwise question their actions if they had not known them.

Hackers/Crackers may break into your systems to simply explore the infrastructure and the systems connected to it or may hack in for malicious reasons.

Industrial espionage involves obtaining confidential data from corporations or government agencies for the benefit of a competing organization. Companies seeking a competitive advantage or governments attempting to assist their domestic industries are the main industrial espionage culprits.

Malicious code refers to viruses, worms, trojan horses, and other "uninvited" software. It not only affects personal computers, which is commonly thought, but also effect more sophisticated systems.

> Virus: A code segment that replicates by attaching copies of itself to existing executables. The new copy of the virus is produced when a user executes the program, such as opening up an email attachment. The virus may contain other malicious code that is triggered when specific conditions are met.
>
> Worm: Unlike a virus, a worm is self-replicating. It does not require a host program. The program creates a copy of itself and executes without user intervention. Worms use network services to propagate themselves to other host systems.
>
> Trojan Horse: A program that was written to perform a desired task, but also includes some hidden functions.

Up until last year the consensus was that more attacks were generated internally rather than externally. The Federal Bureau of Investigations and the Computer Security Institute reported in 2001 that external attacks outnumbered internal attacks for the first time. However it is still believed that internal perpetrators remain the most difficult threats to fight, as they know exactly where the organization's critical information is and often know how to cover their tracks.

Other factors to keep in mind is that far more internal attacks go unreported because companies are able to keep them quiet. Also more companies are employing intrusion detection systems, which let them know they are under attack from the outside. In the past these companies may, and probably were, being attacked but had no way of identifying them.

Vulnerabilities

These threats pose a risk to your organization because they seek to exploit your vulnerabilities.

Your first step should be to determine what the possible vulnerabilities are. A good starting point might be the ICAT Database, which is a CVE Vulnerability Search Engine, a product of the Computer Security Division at the National Institute of Standards and Technology.

ICAT provides a short description of each vulnerability, a list of the characteristics of each vulnerability (e.g. associated attack range and damage potential), a list of the vulnerable software names and version numbers, and links to vulnerability advisory and patch information. You have several search options available to you, so you should be able to pull the exact information you need for the product you are running. As of January 31, 2002, there were 3,526 vulnerabilities in the database.

If you don't want or need to sift through all the vulnerabilities in the ICAT Database, you may just want to review Twenty Most Critical Internet Security Vulnerabilities form SANS. This will give you a good overview of the most dangerous vulnerabilities out there and the ones that are exploited most often. It is broken down into general vulnerabilities that apply to all systems, windows vulnerabilities, and Unix vulnerabilities. There is also a section on the common vulnerable ports.

So far we have discussed vulnerabilities in terms of technical holes in your systems. One of the most critical vulnerabilities in an organization is it's people. Social engineering tactics can be used by hackers/crackers to gain information from authorized individuals thinking they were merely being helpful.

Scanning for Vulnerabilities

Now that you are familiar with the types of vulnerabilities that may be exploitable on your system, you need to scan your system for these vulnerabilities. There are many vulnerability scanners on the market that are designed to assess your network by finding vulnerabilities on your system before they can be exploited. The trick is to select the one that is a good fit for your environment.

The following are some of the more important attributes a scanner should possess:

- An up to date database of vulnerability checks
- Limit the number of false positives
- The ability to store multiple scans and perform trend analysis
- Provide clear and concise instructions for fixing any discovered problem

Now one would expect that these scanners could identify all the vulnerabilities on your system. However, an article in Network Computing Magazine performed a test in a controlled environment to compare the various tools available. Here are some of their comments on the performance of these tools.

Nessus Security Scanner – Identified more vulnerabilities than any other scanner tested and for that reason was rated the top tool. It is an open source tool, as is the architecture for creating the vulnerabilities checks. As you would expect from a free tool, the reporting was not the best.

Axent Technologies NetRecon – The strength of this product lies in the user interface and the backend reporting tool. It did not perform as well as others in discovering vulnerabilities.

Internet Security Systems Internet Scanner – Only Nessus did better on discovering vulnerabilities. The shortcomings in this product were the high number of false positives and inaccuracies.

Network Associates CyberCop Scanner – Identified fewer vulnerabilities than most and had reporting inaccuracies.

BindView Corp. HackerShield – Did a fair job in reporting vulnerabilities, but had false positives also. Proved very difficult to consolidate reporting.

Security Administrators Research Assistant (SARA) – Reported general classes of vulnerabilities. Had week user interface and reporting tools.

World Wide Digital Security System Analyst Integrated Network Tool (SAINT) – Performed much like SARA reporting general classes of vulnerabilities but did not include a reporting tool.

eEye Digital Security Retina – Performed more like a hacking tool performing enumeration instead of looking for vulnerabilities.

Based on the results of these tests, it is safe to say you should not assume you are protected against all vulnerabilities just because your scanner did not reveal anything. That is why it is important to keep up-to-date on the latest information as it is released. Then you can determine at that point if you are affected by a particular vulnerability and take the appropriate action.

Social Engineering

Even if a scanner could identify every technical vulnerability on your system, social engineering could circumvent even the tightest of systems. That is why some people subscribe to the theory that it is poor processes, rather than poor technology that pose the main threat to security.

What is social engineering? It is a term that describes a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures.

The following are some common social engineering techniques, described by nativeintelligence.com, that hackers employ.

Walking into an office and calling out, "I forgot the system password, what is it?"

Walking through offices (posing to be a new employee or repair person or even a documentary film maker) and looking for passwords written on Post-it™ notes.

Calling technical support, giving a user name (from a website, phone book, or papers taken from a dumpster), and asking to have the user's password reset. Sometimes a hacker posing as a user will tell the Help Desk that he or she has an urgent access control problem.

Calling a user and posing as technical support or information services and asking the user for his or her password (often after asking the user if she or he is having trouble with the system and offering to look into it), or asking the user to change his or her password to "debug" their account.

Probability, Impact, and Risk

At this point in the analysis you will have identified all the assets, the threats to those assets, and how they are vulnerable. Now you are faced with one of the most difficult phases of performing a risk assessment. Determining the probability each will occur and what the impact would be if it occurred. The result is the risk associated with the vulnerability.

There are basically two approaches you can take to calculating risk at this point - Quantitative or Qualitative.

The Quantitative approach is not widely used because it involves calculating numerically the probability the event will occur, then assigning a dollar amount to the impact of the occurance. This is extremely difficult. How does anyone know how often someone will attempt a buffer overflow in cb_reset in the System Service Processor package of your SunOS 5.8 that would allow a local user to execute arbitrary code via a long argument. Or, simply assign a numeric value to the probability you will be hacked, period. If you could calculate the probability, your next step would be to assign what the dollar impact to the organization would be if the exploit were to occur. Good luck.

The other approach, and the most widely used form of calculating risk, is the Qualitative approach. This involves subjectively rating the probability and the impact. What you may consider doing is for each vulnerability rate the probability that this may occur as high, medium, or low. Then independently rate the cost this may have on the organization as high, medium, or low. To do this you should solicit input from the business community because in most environments they are considered the owners of the data. So obviously if a particular vulnerability has a high probability of occurring and a high dollar impact if it were to occur, the risk would be considered high.

Mitigation – Technical Countermeasures

Now that we have a risk associate with each vulnerability, the next step is to determine what the possible countermeasures are that will reduce the risk to an acceptable level. From a technical standpoint the possible countermeasures include configuration changes to the system, closing open ports that are not needed, turning off services that are not needed, or installing patches. It is also important at this stage to discuss with the System Administrator the impact any of these changes may have on the system so you can to select the appropriate action. A cost rating should be applied to each countermeasure indicating if the cost of implementing the countermeasure is high, medium, or low.

Mitigation - Security Awareness

As previously discussed, social engineering is a real threat to your organization. It seeks to exploit the actual users on the system. One countermeasure to social engineering is to create a security awareness program so the employees in your organization know what social engineering is and what to look for.

Some issues you may want to address that would mitigate the social engineering risk include:

Password Management – Ensure the users are aware that they should not give out their passwords for any reason. They need to be taught how to create secure passwords, and change them on a regular basis.

Physical Security – Inform employees to not allow individuals to "tail gate" in behind them when entering the building, be aware of individuals wandering around the building without a badge, and to notify building security of any suspicious individuals.

Document Handling – Inform employees of the risks associated with throwing sensitive documents in the trash as opposed to shredding them.

Most important, share stories with the group and give examples of social engineering techniques so the employees can be on the look out for some of the most common techniques.

The cost associated with implementing a security awareness program to address the social engineering risk should be given a rating of high, medium, low.

Mitigation – Cyber Insurance

One mitigation possibility is to obtain a cyber insurance policy. Cyber insurance is a way for companies to mitigate the risks associated with potential losses due to unauthorized access. Some insurance companies now offer policies for hacker intrusions, network downtime, disaster recovery, virus infection, hacker extortion, identity theft, and misappropriation of confidential data.

However since the September 11th terrorist attacks it has become harder to find underwriters willing to issue multimillion-dollar cyber insurance policies. When the policies are written the premiums are usually extremely high.

The Difficulty in Performing a Cost Benefit Analysis

At this point it would be great if you could state to the CIO and CFO, the probability rate that a particular vulnerability would be exploited, the cost to company if it did occur would be $40,000, and the cost to mitigate this risk to an acceptable level is $500. They

would give you the green light to take the appropriate action and mitigate the risk. But as we stated earlier, this is very difficult to do.

The benefits of security have always been a nebulas concept. Avoiding media embarrassment and not being affect by the latest virus are important but they don't translate into profits. The argument we as security professionals usually make is that we have prevented an unknown amount of losses.

Prioritizing and Mitigating the Risk

The information you are armed with at this point should enable you to appropriately prioritize the vulnerabilities. For each vulnerability, you will have a rating for the probability of occurrence and a dollar impact rating of the event, which translate into and overall risk rating. The cost associated with mitigating the risk to an acceptable level has also been rated. You can then begin addressing the high-risk vulnerabilities. Within the high-risk vulnerabilities, you can subjectively determine which to address first based on your knowledge of the vulnerability and the cost associated with mitigation.

Continuous Process

It would be nice if once the initial risk assessment was complete you could just sit back and relax knowing your systems are secure. However, in the changing world of information security, new vulnerabilities are released each day, corporate priorities change, and existing systems are modified. Here are a few processes you should employ to keep up in this fast paced environment.

Keep up to date on new vulnerabilities – You should subscribe to appropriate mailing list so you are made aware of new vulnerabilities as they arise. That way you can evaluate their potential impact to your company and mitigate the risk to an acceptable level immediately.

Perform periodic vulnerability scans – You should scan your system regularly, not just during the formal risk assessment process.

Be involved in new system development - You can safely assume that the sooner you implement security in the life of a system the lower the cost of security will be. The thought being if systems are built with security in mine, it will prevent less work attempting to make changes after the system is in production.

Be involved in the change management process – Systems may change on a daily basis. You should ensure security is considered before any system change is made.

Conclusion

Risk Assessment is an essential part of any information security program and sometimes the most difficult. It should not just be considered the responsibility of the security department. All areas of the information system department must be involved, as should the business owners of the data we are trying to protect. Most of all, Senior Management support is essential to the success of any Risk Assessment Program. And remember, you cannot eliminate risk, only hope to manage it.

Internet Sources

James W. Meritt. "Risk Management"

http://www.auditnet.org/docs/riskmgmt.PDF

ICATMetabase: A CVE Based Vulnerability Database

http://icat.nist.gov/icat.cfm

Fred Cohen, Cynthia Phillips, Laura Painton Swiler, Timothy Gaylor, Patricia Leary, Fran Rupley, Richard Isler, and Eli Dart. "A Preliminary Classification Scheme for Information System Threats, Attacks, and Defenses; A Cause and Effect Model; and Some Analysis Based on That Model" September 1998.
http://secinf.net/info/misc/cohen/cause-and-effect.html

SANS Insitute. "The Twenty Most Critical Internet Security Vulnerabilities (Updated) The Experts' Consensus" Version 2.501 November 15, 2001.
http://www.sans.org/top20.htm

Jeff Forristal and Greg Shipley. "Vulnerability Assessment Scanners" January 8, 2001.
http://www.networkcomputing.com/1201/1201f1b1.html

Peter Coffee. "How to Spot Security Risks" November 19, 2001.
http://www.zdnet.co.uk/itweek/brief/2001/44/management/

Scott Berinato. "Coming Up ROSI" October 26, 2001
http://www.cio.com/security/edit/a102601_rosi.html

Searchsecurity.com. "Social Engineering – A Searchsecurity Definition"
http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci531120,00.html

Nativintelligence.com. "How "Social Engineering" is used to get people to divulge passwords"
http://nativeintelligence.com/awareness/pw-soci.asp

Jay Lyman. “Outside Hackers vs. the Enemy Within: Who's Worse?” February 5, 2002
http://www.newsfactor.com/perl/story/16157.html

Colleen Brush. “CyberInsurance” November 2001
http://www.infosecuritymag.com/articles/november01/industry_cyberinsurance.shtml