Global Information Assurance Certification Paper

GSEC CERTIFICATION PRACTICAL
Version 1.4b

ACHIEVING MANAGEMENT'S SECURITY COMMITMENT

4/1/2003

Sherry Desbrough

ABSTRACT

Spending on information security related technology, training and staff has been inadequate and often non-existent in past years. Although current spending is increasing due to the recent political climate, IT managers could greatly improve their security infrastructures by helping the non-technical senior managers become more aware of potential risks to information. Not too many things will speak louder to senior managers than a thorough risk assessment with the risks expressed in potential dollar losses. This paper will focus on many of the types of risks that Information Technology professionals face, as well as help to develop a risk assessment. A comprehensive risk assessment will not only facilitate the IT area in developing a security program, but will help justify the funds being spent on their security endeavors. A well thought out risk assessment will provide a strong foundation for a reliable security program as well as serve as the foundation for Business Continuity/Disaster Recovery Planning. Anything that can adversely affect the three principles of Information Security (Availability, Confidentiality, and Integrity) is a potential information security risk.

SECURITY STATISTICS

Security incidents doubled in 2001 over prior years and experts believe that incidents will continue to increase at a high pace. As long as organizations continue to develop systems and interconnect them, we will continue to introduce new security issues, vulnerabilities and risks. Unless an organization chooses to keep their computer in the box it came in, locked in a fireproof vault, there will be some risk to the system.

- The 2001 Computer Crime and Security Survey, conducted jointly by the Computer Security Institute and the Federal Bureau of Investigations, shows that 85% of the 538 respondents detected security breaches in the previous 12 months.
- In the same survey, 64% reported financial losses due to computer-related security incidents; 35% of them (186 respondents) were able to quantify their losses in 2001: $377.8 million.
- By contrast, in 2000, 249 respondents said they had lost $265.6 million to security breaches.
- Consultants rank internal breaches at 70 percent to 80 percent of their clients' systems breaches.
- Seventy-nine percent of senior management executives polled by KPMG in 12 countries wrongly believes that the biggest threat to their ecommerce system security is external.
- Nine percent of those polled have had a security breach in the past year, and only 17 percent of those pursued legal action
- Fewer than 35 percent perform security audits on their ecommerce systems, and only half have incident response procedures in place.[1]

The biggest problem with the statistics mentioned above is that they are under-stated. Very few organizations are willing to release information regarding

[1] Mogull

security breaches. They are resistant to providing the public with the information, believing that the public's knowledge of an intrusion could damage the organization's reputation. Customers are often reluctant to do business with an organization that cannot protect their information.

SECURITY AND CEOS/BOARD of DIRECTORS

Implementing a successful security program within an organization, first and foremost, requires top management support and commitment. Implementing a successful security program can be a very expensive venture. Unfortunately, this type of venture does not necessarily add to the bottom line of the organization, thus making it more difficult to obtain management support and commitment. This support and commitment will be much easier to obtain if the risks are well defined, documented and presented to management in a format that makes sense to them.

The current privacy legislation that CEOS and Boards of Directors have to be aware of, such as Gramm, Leach, Bliley in the financial sector or HIPPA in the health care sector, make information security even more critical for management to understand. A company's CEO or Board of Directors could be held liable for unauthorized disclosure of personal non-public information. The reputation of the organization is at risk if the customer base discovers that their information has been leaked or sold without disclosure.[2]

Management is accustomed to their IT department's requests for firewalls and IDS systems to keep the "bad guys" out. They are even going to be familiar with the need for a strict password policy and good internal controls to insure adequate security. Sadly, these countermeasures alone do not provide adequate security for today's information technology climate. We not only need to keep the "bad guys" out, but we need to allow the "good guys" in. We have to make our systems accessible to remote employees or vendors, utilizing VPNs, Extranets and any number of other means of accessing the company's proprietary information. The need for this interconnectivity presents organizations with security risks that management may not be aware of or fully understand. The systems being designed today are being designed to be very open to make the system's usage easier for the end user. This has introduced security vulnerabilities that did not exist in the past. There always seems to be a trade off between ease of use and security.

A well informed senior management will be more supportive of the IT efforts and more willing to allocate the funds to protect the organization's information. Most CEOs and Boards of Directors will be very appreciative of the efforts to keep them informed since they are at risk for very hefty fines and even prison sentences for not complying with privacy legislation. They will also be more willing to provide funding for staff training and services such as penetration testing if they have a full understanding of the risks as well as the consequences.

[2] Hollander

KNOW YOURSELF-KNOW YOUR ENEMY

As stated in the article, Six Top Security Issues for executives: "Sun Tzu, a legendary Chinese strategist born more than 2,000 years ago, taught the importance of knowing both your enemy and yourself:"[3]

If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.

-- Sun Tzu, in The Art of War*, Chapter 3, Verse 18*

KNOW YOURSELF

To accurately access and manage risk, the organization must have an accurate inventory of all information assets that if damaged or disclosed could cause your organization or its employees harm. Many times, there may be someone using an old application that management thought was eliminated years ago. If this application is providing important information, and it is the application is destroyed and irrecoverable-there is risk.

There also may be unsecured modems attached to personal computers. This is one of the most common vulnerabilities in most organizations. Typically, there is no security beyond password security on these modems. All it would take is a script-kiddie with a war-dialer and a password cracker program and they would be on the organization's network in a very short time. These modems could be hiding under a stack of papers or a shoebox without management's knowledge that they are even there. Employees have been known to bring in modems from home and hook them up to bypass perimeter security.

KNOW YOUR ENEMY

You must also know your "enemy". Your enemy can be anyone who could potentially damage your information assets. It may be an external hacker, an unscrupulous business partner, a disgruntled employee or maybe even a well meaning, but under trained employee. Some of your potential enemies would love nothing more than to steal or destroy the assets that you and your organization value, especially if it could bring some type of gain to the enemy.

THE RISK ASSESSMENT

The risk assessment can be an invaluable tool to inform management of potential risks that the company that is in their charge could face. While Information Security, at first glance would seem to be an IT problem, it actually extends to the entire organization. All types of information assets need to be protected whether it is in a digital format, in a paper file or simply residing inside someone's head. In evaluating these risks, it can be very effective to survey as many different people within the organization as possible to gather their ideas of information that could

[3] Hollander

be at risk. Achieving employee buy-in as well as management commitment to security efforts is critical to implementing a security program. An effective way to achieve a high level of employee buy-in is by including them in the process. Talking to people outside of your organization can also be helpful to obtain a fresh prospective on items they view as risks and vulnerabilities.

In addition to surveying the employees of the organization for their ideas of risks, there are numerous vulnerability scanning tools that can be utilized. Most of these tools can be downloaded from the Internet and some can be used at no charge. Intrusion detection software, sniffers and scanners can help you to analyze the traffic on your network. It can help to determine unused services that are running on a system that could be shut down. It is important to keep in mind that these tools are the same tools that can be used by hackers so you want to make sure that you are downloading the tools from a reliable site. You also must be very sure your have written permission to use the tools on the network that you are scanning and probing.

It is important to not limit the risks to digital information. Information is just as private and confidential if it is on a paper document as it is when it is in a digital form. It may even be more at risk if it is something that cannot be reproduced or if it is easily accessible by an unauthorized person. There could be an important document stored in a file only on company premises. If there is a fire, that document is gone forever. This is a risk. Imagine an employee who has a critical procedure stored in their brain. Maybe they have been with the organization for years and they are the only one who even knows that they do this procedure. This is a risk to the information that the person holds in their brain.

ASSESSMENT PROCESS

A format that is very easy for non-technical management to understand is a simple grid listing the risks, their threat, likeliness of occurrence, etc. A severity should be assigned to each risk as well as a likelihood of the risk occurring. There is an equation for calculating the severity of a computer breach that can be used. The formula is "severity = (criticality + leathality) – (system countermeasures + network countermeasures)".

A short description of the current countermeasure should also be included if there is one in place. Another item that should be included is the cost of incurring the risk. The following formula can be used for calculating risks.

RISK = ASSET VALUE X THREAT X VULNERABILITY

This makes the assessment very meaningful to the managers who have to make a decision on whether to spend funds for the protection. There are several action plans that an organization can choose to do once they know the risks involved.

- Accept the risk (Acknowledge the risk but do nothing)
- Mitigate the risk (Implement Countermeasures)
- Transfer the risk (Insurance)

If the cost of incurring the risk does not outweigh the cost of mitigating the risk, management will undoubtedly decide to accept the risk and hope for the best. If the cost of the risk is higher than the cost of protecting from the risk, smart management will probably allocate funds to protect from the risk. They may also decide to transfer the risk to an insurance company.

How an organization values their assets is an individual preference and usually the most difficult part of the risk assessment. Some factors that can be calculated are downtime, loss of revenue, and actual loss of the asset. Other costs that are more difficult to put a dollar figure on are loss of customer confidence, damage of reputation, loss of proprietary information and possibly even bankruptcy. As an example, backup media is very inexpensive; the value of the data on the media is very valuable.

Another asset that cannot be forgotten is the human asset. People are, after all, the most valuable asset to an organization and human safety is always considered to be the number one priority. It may be a risk to an organization if several key employees were to take a single flight to a conference. If the plane were to crash, it could have a significant impact on the organization. The cost of losing a valuable person that has years experience can be a significant risk. One only has to remember back to September 11, 2001 to understand the implications of the loss of people. It is difficult to fathom the human asset loss from the Cantor Fitzgerald Company which lost 2/3 of their 1000 employees in one day.

There can also be different types of threats for each asset. An asset can be damaged, it can be stolen, disclosure of private information or unauthorized alterations can be made to name just a few. There may need to be countermeasures, risk acceptance, or risk transfer for each type of threat that you choose to address. Sometimes one countermeasure will serve to protect assets from many different risks. Sometimes one countermeasure will only protect one asset. As an example, fire suppression will prevent the computers from burning but it won't help much if someone walks out of the building with them.

The team performing the risk assessment may be tempted to make every asset a high priority and to recommend strict countermeasures to protect every asset. This would be an easy way to make sure every information asset gets the protection resources that it requires but not very practical. It would be very costly and almost impossible to treat all assets as though they are the most important. Usually, there will not be enough financial and human resources to protect all assets equally. There will need to be some prioritization done in the assessment to determine what information assets to protect and which assets to accept or transfer the risk.

The countermeasures put in place must also be user friendly to the people who have to use the system. They must also be mandatory. It cannot be left up to the users discretion to bypass the security systems that have been put in place. The

countermeasures cannot be so secure that no one can use the system. I.e. Passwords should be strong but not so difficult that users write them down and attach them to their monitors because they cannot remember them. This will only cause unnecessary grief to the user as well as the IT department and maybe even facilitate attacker access.

SAMPLE RISK ASSESSMENT DOCUMENT

Legend:
1=Low
2=Medium
3=High
4=Very High

Asset	Asset Value	Threat Type	Threat	Vulnerability	Risk	Countermeasures
Personal Computers-each	1,500.00	Theft	3	2	9,000.00	Laptops use locking mechanisms. Some risk is transferred to insurance company. Unauthorized people not allowed in area of computers
	1,500.00	Hardware Failure	4	2	12,000.00	Critical data is saved nightly to tape; certain necessary programs are installed on a second pc for disaster purposes.
	3,000.00	Virus	4	4	48,000.00	4 hour unattended, mandatory check for update/update of virus signatures
Computer Monitors	250.00	Unauthorized Viewing	3	2	1,500.00	Monitors turned away from public view, screen saver with passwords, 15 minute timeout on inactive displays.
Backup Media	100,000.00	Loss	2	2	400,000.00	Logged and kept offsite
	100,000.00	Theft	3	3	900,000.00	Locked in a safe in a locked room
	100,000.00	Fire	4	4	1,600,000.00	Backup copies, offsite, fire proof bag for transport
	100,000.00	Spoilage	3	3	900,000.00	Replace tapes on yearly basis or more if errors are occurring
Paper Files	500,000.00	Theft	4	4	8,000,000.00	Locked in a safe in a locked room when possible
	500,000.00	Unauthorized Viewing	2	3	3,000,000.00	Kept in locked rooms until shredded. Someone oversees shredding process when done by 3rd party.
	500,000.00	Loss	3	3	4,500,000.00	Documents must be imaged
	500,000.00	Fire	4	4	8,000,000.00	Documents must be imaged
	500,000.00	Flood	1	1	500,000.00	TBD

AREAS OF SECURITY RISKS

There are six primary areas of concern with systems security risks.

- Data Privacy and Confidentiality
- Data Integrity
- Data Availability
- Authentication
- Non-repudiation
- Access Control/System Design

Data privacy and confidentiality means that data is only viewed or accessed by the person who is intended to view or access it. When assessing issues regarding data privacy and confidentiality it is important to evaluate digital assets as well as non-digital assets. It doesn't help a company's information security posture to have high tech systems in place to prevent disclosure of customer's account numbers if a user tosses old reports in the trash without shredding or if the user walks away from a monitor in public view without initiating a password protected screen saver.

Data integrity means that the data has not been altered or damaged in any way that it should not be. The integrity of data can be negatively affected in many ways. A malicious intruder could access a website and change information to mislead unsuspecting web browsers or an under-trained user could make an error that could damage the integrity of the data.

The availability of data means that it is there and ready to be accessed when it needs to be accessed. The availability of data could be adversely affected by a system failure. Having very important data contained on a machine without RAID protection would be a risk. Not having backup lines for data circuits would be a considerable availability risk if the circuit were to go down.

Authentication controls are necessary to establish the identities of all of the parties to a communication. It is very common for someone's identity to be misrepresented by a person coming from a compromised host pretending to be somebody legitimate, or making email seem as if it came from someone else. Just as common, is a person placing a call to a company, requesting account information. They can easily lie about their identity to obtain account information for malicious purposes. This is referred to as social engineering and is undoubtedly one of the most difficult risks to consistently mitigate due to most people wanting to be helpful and the lack of security training.

Non-repudiation involves creating proof of the origin or the delivery of data to protect the sender against false denial by the recipient that the data has been sent. An example of non-repudiation in a non-digital format may be a proof of delivery receipt from a shipping carrier. Using digital signatures such as PGP can provide non-repudiation for an email message.

Access controls and system design determine how a user would access the system and how the organization controls such access. Logical access controls include user IDs and passwords, access lists and any other means of controlling access through software. Physical controls could involve the locking of computer rooms and wiring closets, fire protection in computer rooms, authorizing only necessary employees to certain areas.

Regardless of whether a security concern is abused intentionally by a malicious hacker or inadvertently by an under trained user, the results can be the same. The organization's integrity and customer information could be at risk. This

makes it crucial that a risk assessment not only include digital risks but non-digital as well.

Once there is a thorough understanding of the areas of risk that the organization can encounter, it is important to understand the major risk vectors that could affect information security.

MAJOR RISK VECTORS

- Internal Risks-Intentional
- Internal Risks-System Misuse
- Internal Risks-Inadvertent Misuse
- Internal Risks-Software Piracy
- External Risks-Hackers
- Physical Risks such as fire, flood, tornadoes, and etc

INTERNAL RISKS-INTENTIONAL ATTACKS

As stated earlier, it is estimated that 70-80% of all information security risks are internal to the organization. While this number is widely disputed, internal attacks may actually be a much lower percentage of total risks but much higher in financial damages. Disgruntled employees account for a large percentage of internal attacks. Employees are also very familiar with the information assets of the organization that they work for which makes compromising them much easier. Management has always believed that the biggest threats to their systems were the "black hat" hackers and that a good firewall was a good security program. These statistics seem to tell that a good firewall is only a small part of overall security.[4]

In the "old days" IT was centralized, thus security was centralized. It was very easy to contain users. With the addition of personal computers to every desk, the security culture changed immensely. Not only does every desk have a computer; but almost all employees have at least one computer at home. These home users tend to become much more technically savvy. This new technical savvy introduces new security risks. It is often said, "A little knowledge is dangerous." There seems to be a limitless number of things an internal attacker, who is trusted by the company could do.

- Installation of a logic bomb by a discharged employee
- Unauthorized access and disclosure of sensitive information
- Unauthorized access for later extortion purposes
- Equipment theft
- Intentionally failing to follow procedures
- Deleting information
- Creating a backdoor entrance point into the system for later use
- Information theft for sale or personal use
- Trade secret theft and/or sale
- Information theft/access by contractor or authorized vendor

[4] Scallet

INTERNAL RISKS-SYSTEM MISUSE

Another contributor to internal attacks is an employee who abuses his privileges and uses the system for purposes other than what it is intended for. These risks can cause harm by utilizing excessive bandwidth, introducing harassment issues to other staff, opening the doors for viruses among a multitude of other potential threats. These types of risks can either come from the general employee population of the organization as well as information technology employees. An employee may perform a misuse attack without fully understanding the consequences thus making this is an area where policy enforcement and training can help to reduce the risks. Some examples of system misuse are:

- Accessing inappropriate websites
- Using email for spam or mailing lists such as jokes and chain letters
- Downloading music and other media that utilized excessive bandwidth
- Utilizing chat rooms during work hours
- Leaving sensitive information in public view
- Allowing read access to upload FTP sites thus becoming a repository for pirated software
- Failing to perform backup procedures
- Sending non-encrypted confidential information
- Not allowing virus signature updates
- Allowing obsolete user ids to remain on system
- Not securing a wireless network properly
- Assessing an internal network from home without adequate virus protection and security controls in place

INTERNAL RISKS-INADVERTANT MISUSE

Probably one of the most difficult contributors to internal system problems is inadvertent misuse of the system. This type of misuse that causes risk can be performed by the general employee population or by information technology employees. This generally is indicative of a much larger problem and that is lack of user training.

- Inadvertent destruction of backup media
- Deleting files
- Accessing and executing programs that should not be run
- Opening dangerous email attachments
- Not keeping system current with security patches
- Keying errors
- Accessing confidential information

SOFTWARE PIRACY

Software piracy might not be found in all risk assessments but when one thinks of the risks to the organization if they are found to be in violation for licensing agreements, it would make sense to address it in the risk assessment. Organizations risk very large fines, damage to reputation and even imprisonment for these violations. Using pirated software can also be a contributing factor for

the introduction of virus's or other malware into the system, which does pose an information security risk.

EXTERNAL ATTACKS-HACKERS

Management will be most familiar with external attacks because the attacks that do make the papers are usually attacks from hackers. These attacks can come in many forms and can be performed for a variety of reasons. It may be to disrupt your business, to obtain confidential information or possibly just for entertainment. Some of the attacks that are performed by an external hacker are as follows:

- Denial of service
- Sending viruses and worms
- Defacement of web sites
- Stealing confidential information for personal gain, i.e credit card accounts
- Password cracking

All of these risk vectors can cause significant harm to an organization's information assets but it is generally a rare CEO that would be fully aware of all of these possibilities. Generally, all of the focus has been to protect the perimeter of the network and the physical risks that non-technical managers understand.

Once the risk vectors and individual risks have been identified, countermeasures need to be researched and recommendations should be made for each risk or group of risks as well as costs associated with the countermeasures. The evaluation of each of these risks will make formulating your security programs and business recovery plans a much easier task. The costs of potential risks being well documented will give validity to the IT department's request for funds to help mitigate the risks.

MITIGATION OF RISKS

Once risks have been identified and quantified, it then becomes much easier to go through the assessment with senior management and make sure that you have an action plan for each item in the assessment. The organization may find that one asset is far too costly to protect while another is too costly to not protect. It is wise to put the action plan of each documented risk in the assessment. If the organization is going to accept the risk it may be very helpful to have that decision well documented as well.

EDUCATION

After all the risks have been assessed, the finances have been obtained, the countermeasures and security systems put in place; it is critical that users are fully trained in the policies and procedures that have been developed. Issues such as Social Engineering need to be continually reinforced to make sure users never let down their guard. Security issues not only need to be continually reinforced but continually tested. Routine penetration testing should be done by the IT security specialists as wells as periodically testing by an independent third party. This is a good way of achieving objectivity in the systems designed. Please

keep in mind to ALWAYS obtain written permission prior to conducting any type of penetration testing.

SUMMARY

Always remember, communication is a key component to keeping our information safe. Management needs to know and understand the risks, IT has to keep the lines of communication open when addressing risks and the users need to be educated and re-educated on the risks. There is one very important concept to keep in mind. When your risk assessment is complete, you must do a risk assessment! In other words, this process is never complete. As your systems are constantly evolving, so are the risks. It is truly a journey-not a destination.

WORKS CITED:

Hurley, Edward. "CSI: Examining threats from inside the firewall." 14 Nov 2002. URL: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci863439,00.html

Fisher, Vivienne. "Security holes: The danger within." 12 June 2002. URL: http://www.foundstone.com/newsletter/sep-02/ask_the_expert.html

Mulcahy, Ryan. "Global Crossing employee data exposed on the Web." 12 June 2002. URL: http://www.gartnerg2.com/research/rpt-0102-0010.asp

Mearian, Lucas. "Managing Financial Services Security: An Internal Affair." 05 Aug 2002. URL: http://www.computerworld.com/industrytopics/financial/story/0,10801,73167,00.html

Jupiter, Olaf. "Executives unaware of internal security risks." 21 Nov 2001. URL: http://www.e-gateway.net/infoarea/news/news.cfm?nid=2026

Hollander, Yona. "Six Top Security Issues For Executives." 30 Dec 2002. URL: http://www.computerworld.com/securitytopics/security/story/0,10801,77132,00.html

Tickle, Ian. "Snapshot for Security". Jan 2003. URL: http://www.infosecnews.com/opinion/2003/01/15_04.htm

Mogull, Rich. "Building a Security-Aware Enterprise". 17 Jan 2002. URL: http://www.gartnerg2.com/research/rpt-0102-0010.asp

Scallet, Sarah. "Dr. Crime's Terminal of Doom." 01 Jun 2002. URL: http://www.cio.com/archive/060102/doom.html