Global Information Assurance Certification Paper

The Human Factor

By Eric Padilla

Introduction

The security environment in which we live is very dynamic and uncertain, replete with numerous security challenges. Information technology is gaining in importance everyday, as its use becomes mainstream in governmental operations and commercial markets and although it is a truism to state that IT today is beyond rapid evolution and is in fact in a state of explosive evolution. This new technology has not only bought great advancements to society but in addition presents a diverse set of threats to our ongoing goals and security.

The annual CSI / FBI computer crime survey published in the spring 2001. The respondents included 583 organizations, which included government, finance, health-care, and academia. The total reported losses were $377M. About 85% of the respondents experienced breaches of information security in the preceding 12 months; the top three problems were computer viruses, laptop theft and employee net abuse. However, 70% of the respondents also reported other types of breach: theft of secrets, financial fraud, outsider penetration of security perimeters, denial of service, and sabotage of data or networks. Some 70% of the respondents also rated the Internet connections as a more frequent point of attack than internal systems.

The above statistics are very alarming; it is evident that humans are key to ensuring that computer resources and information are protected. However, they are also the source of most of the security problems.

Malicious Insider

On July 30, 1996, a computer time bomb was unleashed, deleting and purging Omega's most critical manufacturing programs. The consequences for this high-technology company were enormous - upwards of $10 million in damage and lost productivity.

Mr. Tim Lloyd, a former network administrator at Omega Engineering Corporation, developed a software time bomb, which was unleashed after he was fired for performance and behavioral problems. This Mr. Lloyd was a trusted employee for 11 years.

Industry analysts estimate that internal security breaches account for approximately fifty percent of the attacks on corporate computer networks. And the percentage is probably even higher than that because most insider attacks go undetected.

Security control must be carefully designed, deployed, and maintained to protect systems from the insider threat.

- Implement **Two-Factor Authentication**

  Passwords are the traditional method to authenticate users to computer systems; significant number of computer break-ins can be traced back to the use of passwords. Passwords are vulnerable to dictionary attacks, brute force attacks, social engineering, and users written them down. Passwords alone offer an insufficient defense.

  Two-factor authentication is a method of positively identifying a person. Two factors in two-factor authentication are:

  - Something you have—including keys or token cards.
  - Something you know—including passwords.
  - Something you are—including fingerprints, voiceprints or retinal scans.

- Conduct vulnerability scans to uncover any weaknesses or holes in your networks and systems.
- Institute the *Separation of Duties* concept to ensure that one individual does not have access to the whole network.
- Conduct background checks before hiring employees. This is an attempted to selected trustworthy individuals.
- Install a reputable virus-scanning program. Installing a virus detection program is not enough. Make sure to follow the vendor's instructions for updating the "virus signature file" periodically.
- Enable auditing to log access attempts and refusals to sensitive data. Audit logs are used after the fact to analyze various security events. Logging access attempts and refusals provides the ability to review what users are trying to access.
- Develop and implement a Disaster Recovery Plan. Mission critical information must be backup and verified to ensure information has been saved correctly.

Outsider

In 1992, Kevin Mitnick, "America's Most Wanted Computer Outlaw," was charged with a violation of his supervision. He went underground and online, using the Internet to crack computers belonging to such cell phone and computer makers as Motorola, Fujtsu and Sun Microsystems and to copy more proprietary source code. The FBI captured him on Feb. 15, 1995.

With the advent of the Internet, and each year more people around the world have access,

security breaches from the outside are on the rise. Especially with open source tools available on the Internet, anyone who has a connection to the Internet has the ability to ric havoc on the World Wide Web. The skill level or the age of the person using the tools is not a factor. It can be a 10-year-old kid who is curious, and with these new Graphic User Interface (GUI) tools, all someone has to do is point and click.

This means as a security professional, security barriers, also known as "Defense in depth", need be properly planned and implemented to ensure internal system are protected against unauthorized intruders.

- Install a firewall between the internal network and the Internet. A firewall monitors data coming into and going out. It reads the identity of each computer that sends data, comparing each ID to a list of trusted computers. If an outside user tries to log into the system from a computer that the firewall doesn't recognize, the firewall keeps the outsider from accessing the system.
- Deploy host and network-based intrusion detection tools and monitor results on a daily basis. Network- or a host-based approach attempts to recognize attacks by looking for ***attack signatures***, specific patterns that usually indicate malicious or suspicious intent.
- Implement a reputable encryption program. Even if an intruder manages to break through a firewall, the data on a network can be made safe if it's encrypted.
- Don't allow users to run downloaded 'exe' files. Not allowing users to execute downloaded executables will minimize the potential of a Trojans entering a system.
- Set permissions so that users cannot modify system files. This will prevent users from be able to corrupt or change system files.
- Run anti-virus software on all your computers. Anti-virus software scans a system for virus, worm, Trojan, etc. This software prevents a system from being infected.
- Limit access to the administrator/root account. Since having access to the administrator or root account gives you "keys to the kingdom", every effort should be made to reduce the amount of people who have access to these accounts.

Negligence

Humans inevitably make or break a computer security program. Human actions account for a majority of computer-related losses than all other sources. Humans are, by nature, imperfect. Technical solution cannot solve every security problem because users never do what the designers expected. Humans tend be very curious and some are oblivious.

The types of human activities that cause majority of the losses are errors and omissions. How do you minimize loss caused by a negligent user?

- Develop a corporate security policy, which documents corporate computer security

decisions: resource allocation, competing objectives, and organizational strategy related to protecting both technical and information resources as well as guiding employee behavior.

- Develop a computer security training and awareness program. All users must be trained on their responsibilities and the proper use corporate computers prior to receiving access to any computer resource.
- Develop policies and procedures identifying responsibilities and consequences of non-compliance
- User must knowledge their responsibilities by signing a rules of use form.
- If all else falls use the FUD Factor (fear, uncertainty and doubt). Fear can be a good short-term motivator.

Theft

Investigators arrested several former IBM employees and a Georgia businessman in connection with the theft of more than $20 million worth of computer parts form a NY IBM plant. The suspects allegedly transported more than 3000 stolen memory cards by and selling them to black marketers. They are charged with laundering more than $700,000.00 in profits from the illegal sales through computer companies.

Computer theft is a serious problem in North America, which exceeds approximately $3 billion each year. One of the most popular targets is the laptop.

Laptops are not only susceptible to theft and loss, but they are also very prone to damage. Most laptops are stolen from the office, hotels and airports.

There are some "best business practices" that may prevent the theft of laptops or help in their recovery. Some of these are basic and others require a more physical or technological approach to the issues.

- Keep your laptop with you at all times. Don't leave a laptop visible or unattended.
- Keep your laptop in a brief case or other plain bag. Laptop cases designed clearly portray their contents, making it an easier task for the thief to spot in a crowd. The case containing the laptop should be locked with a simple luggage lock to provide additional protection.
- Going through a security checkpoint in the airport, wait to the last possible moment before placing your laptop on the x-ray conveyer— if possible, just as you are about to pass through the metal detector. Be alert of your surrounding; if someone in front of you sets off the metal detector, delaying your progress, could be an indicator that someone has targeted your laptop at the end of the conveyer.
- If you leave your laptop in your room, store the computer away in your luggage along with peripherals or other revealing indicators of a laptop and lock all your luggage items.
- Use an encryption program to prevent unauthorized access to corporate information on your laptop.

Conclusion

Computer Security (CS) continues to have a tremendous impact on management and organizations. Managerial responses to CS have influenced strategy, altered structures, reshaped communication and learning, as well as organizational design. In today's, rapidly changing Information Technology (IT) environment, and not clearly understanding the role of CS within an organization could be extremely costly. Manager will be unprepared to make the appropriate decisions for the 21st century.

The surge in information technology during the latter part of the 20th century has forced organizations to meet its security challenges with an increased in funding and information resources.

It would seem that business investment in CS is at root no different from business investment in anything else. After a careful consideration of the costs of the investment and its anticipated benefits, a decision has to be made as to whether the benefits of the investment outstrip the costs and by how much. If the benefits are competitive with other investment alternatives, then the business will commit financial resources to the CS proposal. Otherwise it won't.

The security strategies identified are not all inclusive. Every situation is different, and not all solution fit the situation. Several other factors play role in determining what security solution(s) need to implemented: environment, people, funding, and technological resources. It is very important during the planning stages that security solutions selected truly resolve a problem(s).

References

Computer Security Issues & Trends: 2001 CSI/FBI Computer and Security Survey

Computer Security Journal Volume XV, Number 1, Winter 1999

Computer Security Journal Volume XV, Number 4, fall 1999

Micki Krause, Harold F. Tipton (Editor): Information Security Management Handbook, Fourth Edition

Deborah Russell, J T Gangemi: Computer Security Basics, 1992

David Icove, Karl Seger, William Vonstorch: Computer Crime : A Crimefighter's Handbook

Vince Tuesday: Human Factor Derails Best-Laid Security Plans, April 30, 2001

Sydney Herald 20/07/1999 :"Building Barriers Against Hackers"
http://www.infowar.com/hacker/99/hack_072199c_j.shtml

Actual Crime Stories
http://www.lightguardian.com/crime_stories.htm

Human error: the source of most security problems, 1995-2001 Network World
http://www.nwfusion.com/columnists/2001/00379820.html

An Introduction to Computer Security: The NIST Handbook
http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf
http://csrc.nist.gov/publications/nistpubs/800-14

Computer Security Institute
http://www.gocsi.com/prelea/000321.html