CIS 333

Week 4 Assignment 1 Submission

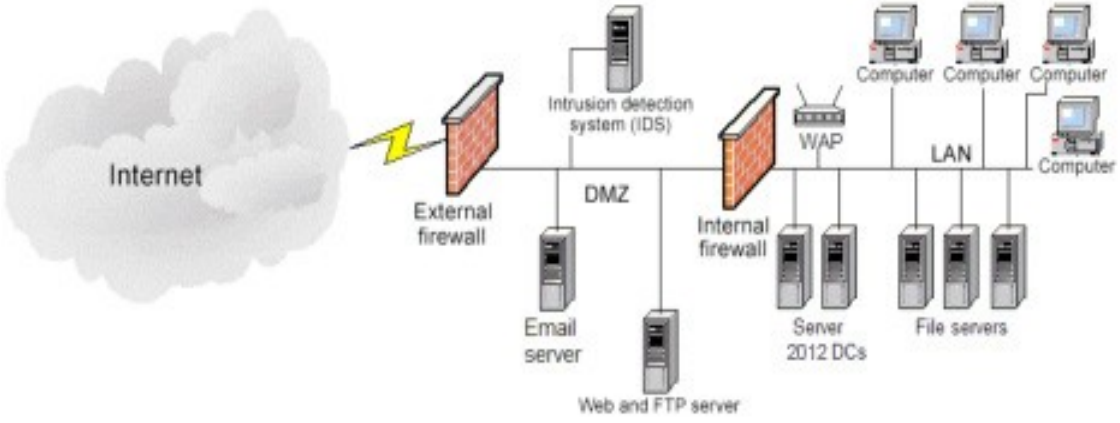
Assignment 1: Identifying Potential Malicious Attacks, Threats and Vulnerabilities
Due Week 4 and worth 75 points
You have just been hired as an Information Security Engineer for a videogame development company. The organization network structure is identified in the below network diagram and specifically contains:

1) 2 – Firewalls

2) 1 – Web / FTP server
3) 1 – Microsoft Exchange Email server
4) 1 – Network Intrusion Detection System (NIDS)

5) 2 – Windows Server 2012 Active Directory Domain Controllers (DC)
6) 3 – File servers
7) 1 – Wireless access point (WAP)
8) 100 – Desktop / Laptop computers

9) VoIP telephone system



The CIO has seen reports of malicious activity being on the rise and has become extremely concerned with the protection of the intellectual property and highly sensitive data maintained by your organization. As one of your first tasks with the organization, the CIO requested you identify and draft a report identifying potential malicious attacks, threats, and vulnerabilities specific to your organization. Further, the CIO would like you to briefly explain each item and the potential impact it could have on the organization.
Write a four to five (4-5) page paper in which you:

1. Analyze three (3) specific potential malicious attacks and / or threats that could be carried out against the network and organization.
2. Explain in detail the potential impact of the three (3) selected malicious attacks.
3. Propose the security controls that you would consider implementing in order to protect against the selected potential malicious attacks.
4. Analyze three (3) potential concerns for data loss and data theft that may exist in the documented network.
5. Explicate the potential impact of the three (3) selected concerns for data loss and data theft.
6. Propose the security controls that you would consider implementing in order to protect against the selected concerns for data loss and data theft.

7. Use at least three (3) quality resources in this assignment (no more than 2-3 years old) from material outside the textbook. Note: Wikipedia and similar Websites do not qualify as quality resources.

Your assignment must follow these formatting requirements:

- Be typed, double spaced, using Times New Roman font (size 12), with one-inch margins on all sides; citations and references must follow APA or school-specific format. Check with your professor for any additional instructions.
- Include a cover page containing the title of the assignment, the student's name, the professor's name, the course title, and the date. The cover page and the reference page are not included in the required assignment page length.

The specific course learning outcomes associated with this assignment are:

- Explain the concepts of information systems security as applied to an IT infrastructure.
- Describe the principles of risk management, common response techniques, and issues related to recovery of IT systems.
- Describe how malicious attacks, threats, and vulnerabilities impact an IT infrastructure.
- Explain the means attackers use to compromise systems and networks, and defenses used by organizations.
- Use technology and information resources to research issues in information systems security.
- Write clearly and concisely about network security topics using proper writing mechanics and technical style conventions.

Potential Malicious Attacks and Threats

Assignment 1: Identifying Potential Malicious Attacks, Threats, and Vulnerabilities
Shauna
Video games have been around for many years. As technology progresses unfortunately so does the security risks that come with online gaming. “The number of American households which play video games is a roughly 65%.” (Source 2)
With any network organization you want to make sure that you keep on top of vulnerabilities of anything that reaches out to the internet. Computers and servers that touch the internet are ones that must be scanned. As a company you have to make sure that you configure the security settings for the operating system, internet browser and security software. As a company you also want to set personal security policies for online behavior. There also needs to be an antivirus installed on the network like Norton or Symantec which blocks threats targeting the vulnerabilities.
“With the firewalls you want to configure them in the reputable internet security program to block unsolicited request communication.” (Source 1)
Email server needs to be sure that spam doesn’t get through the network. The ways that spam works is unwanted email messages get solicited to a large number of recipients. “Spam should be a major concern in your infrastructure since it can be used to deliver email which can include Trojan horses, viruses, worms’ spyware and targeted attacks aimed specifically in obtaining sensitive and personal identification information.” (Source 1) Microsoft Outlook has some known security risks. However, “most of the security configurations would be set on the Exchange server and passed down to all clients.” (Source 2)

With the organization running Windows 2008 domain controllers with an integrated Active Directory and an Exchange server for email functions, “there are risks associated specifically to those types of operating systems.” (Source 2) If you do not keep on top of the systems and do the necessary patches regularly there could potential security risks. (Be sure that you are not just installing any patches because implementing an untested patch could potentially bring down the servers.) You must also “configure security settings for your operating system, internet browser and security software.” (Source 3) “The other thing to think about with Microsoft servers is that known viruses and malware is designed and created to specifically target Microsoft systems.” (Source 2) Flaws like these that “these mistakes include weak/default passwords, ports left open, permissions left undefined, an unprotected directory that anyone with a bit of knowledge can access and rewrite, and more.” (Source 3)

To protect the infrastructure you can install spam filtering or blocking software otherwise keep your employees up to date on how to handle spam –like if an email comes in and does not have your email address in the TO or CC fields mark it as spam and do not open that email.
As with all video gaming companies there are a variety of different networking devices which is usually Cisco or other networking manufacturers. “Most companies are usually comprised of a fully functional TCP/IP network, where larger companies would be comprised of a WAN network.” (Source 2)

The need to have a network intrusion system is both evident and very important for an integrated infrastructure. With this type of system in place it would help to “detect and prevent lost information including names, addresses, email addresses, gender, birthdates, phone numbers and login information.” (Source 2)
Programming languages such as C++, Java and C# to name a few, have their own security risks within the enterprise that can create risks whenever they are used. “A common place for .Net is throughout the various websites that video game company’s use.” (Source 2) This is a risk because if a hacker gets through they can steal usernames and passwords this can be likely

accomplished by the hacker accessing the websites to access either a “MS SQL server database and or a SharePoint database.” (Source 2)
As far as security policies are concerned the main ones that need to be created and addressed are: “enterprise information security policy (EISP), issue-specific security policy (ISSP), and a systems-specific policy (SysPS).” (Source 2) The first EISP is to provide in details the stance the company has on security. This should also include the responsibilities that are required to ensure the safety and security measures of the organization. “An ISSP would cover things like authorized access, equipment usage, and systems management.” (Source 2) The SysPS this would include anything else that company needs to cover and have in written format.
Information assurance is also very important to mention in a video game company. You definitely want to make sure that the systems have the availability to be redundant. You can do this by creating a RAID 5 system in each of the servers. “This becomes redundant because if one drive crashes then a new one can be replaced. This allows the video game system to remain operational as long as possible” (Source 2) Also, if something were to happen to the RAID 5 the system could still remain operational. Something else that you may want to consider is cloning the servers at multiple locations. “The most common type of cloned server would be the domain controllers. File systems can also be cloned as well.” (Source 2) Having this information in 2 different places creates the redundancy as well and can also backup data.
This information should stand as a good starting point for any video game company. The most important thing to remember is that technology changes all the time and in order to keep informed and on top is to always be doing research. Being aware of updates, vulnerabilities and patches will always help your infrastructure. Building on that and using VMware servers and cloning other servers or domain controllers are always going to have you a step ahead of any hacker. “Addressing the security issues and implementing the security controls today will only strengthen each company tomorrow.” (Source 2)

References
http://hiring.monster.com/hr/hr-best-practices/monster-training/security-center/avoid-computer-threats.aspx
http://arxiv.org/ftp/arxiv/papers/1111/1111.1769.pdf
http://www.slideshare.net/rudrak/security-threats-for-online-game-portals

Identifying Potential Malicious Attacks, Threats, and Vulnerabilities

For a better understanding of the situation in the network of the company I decided to start the analysis by the vulnerabilities that this one presents. Many of these vulnerabilities are the cause for different types of network attacks. It should be noted that while many of these vulnerabilities may be mitigated or eliminated the possibility of an attack always exists.
The first vulnerability is the email server. Although very well controlled for been within the Demilitarized Zone (DMZ), this is always a vulnerability with which most companies have to deal with. This vulnerability opens the way for phishing attack. One way to mitigate this vulnerability is configuring the email server so that only authorized email may enter. This is difficult because our video game company has a large list of customers and suppliers that are in constant change. The best option is to alert users about the security measures and company policies regarding private and unknown emails.
The Web and FTP server can be a not very alarming vulnerability. Because it is located in the DMZ and after the Intrusion Detection System (IDS), is unlikely to be corrupted without being detected.

The location of the file servers in the network is totally unprotected against internal attacks. Any successful attack in the LAN would leave the data servers exposed. The establishment of a demilitarized zone with a completely different set of log on names and password than any other machines would give these servers better security. The LAN can be compromised but the data still remain in a safer area of the network.

The most vulnerable point of our network is the Wireless Access Point. It is located inside the LAN, which reduces network security, being away from the protection of firewalls. The only protection it has is the internal configuration. This vulnerability provides various attacks like Snooping, Brute-Force and Eavesdropping. Do not think it's necessary to have a WAP in the company but if necessary I suggest that should be installed inside the DMZ, after the external firewall, IDS just before, if someone unauthorized gets through it will be detected and we have the safety of the internal firewall.

Let's analyze the various attacks and threats to which our network can be a victim. For a better understanding I'll start from the most external layer of the network.

Phishing or Spear Phishing is an attack that may be carried through the email server. In this attack the hacker creates a fake web site that looks exactly like a popular site or any of ours providers / clients. The purpose of this attack is to collect sensitive information about users or the company. An attack of this type may be little detrimental or devastating, depending on how much and how important is the information collected. If this information provides access to the network to an unauthorized person we could be facing the three types of threats: Denial or Destruction, Alteration and Disclosure. It all depends of the intentions of the attacker.
The WAP can be a victim of multiple attacks. Eavesdropping is one of the most common attacks made against this type of device. Such attack can read and capture all types of packets transmitted through a network. Due to the location of the WAP our main threat would be disclosing of classified information to other sources.

The second most common attack facing us in this segment of the network is Brutal-Force. This attack is based on trying all possible combinations and password to break the security. With the power of modern computers no matter how good the password, eventually all possible combinations will be tested. If this attack is successful, the attacker has access to the internal network of the company so in this case we can be under the three types of threat; it all depends on the intentions of the attacker. The most advisable is to change the password at least every 30 days and if possible relocating the WAP to a most protected location of the network.

Another possible attack that we can face when dealing with WAP is Address Spoofing. This attack consists of trying to seem at something that really is not. Is normally present a false network address to pretend to be an authorized machine of the system. If the WAP is not configured to filter out traffic with internal external addresses, the attack may be successful. The main objective of this attack is the destruction and / or alteration of the system and the information; although it remains the possibility of disclosure.

The last segment of analysis is the one were the users and data servers are located. The only visible attack in this area is Insider Attack. This type of attack is usually carried out by disgruntled or corrupt employees to take advantage of a situation. Although on a smaller scale, is always present in all companies and is more difficult to detect because the attacker has access to the system without having to perform any suspicious operation.

Eavesdrop, steal, or damage information, use information in a fraudulent manner, and deny accesses to other authorized users are the most frequents procedures performed in such attacks. One way to reduce this attack is by correctly setting Discretionary and Mandatory Access Control. In this way if a user attempts to perform an Insider Attack their access to information will be limited and at the same time it is easier to identify the source of the problem.

From this attack can be derived also a Social Engineering Attack. Some users with limited access to resources and system data may try to make another with a higher access level to provide information or grant him access to prohibited areas.

Due to the above I recommend a restructuring of the company network. Many attacks, threats and vulnerabilities previously analyzed are due to problems in the network configuration. In a same way it should be review the internal configuration of each device, access controls and permissions for groups / users to ensure maximum security.

References

Network Security (n.d.). In Computer Networking Notes online. Retrieved from http://computernetworkingnotes.com/network-security-access-lists-standards-and-extended/types-of-attack.html/

How to Design a Secure DMZ (n.d.). In eWeek online. Retrieved from http://www.eweek.com/c/a/Security/How-to-Design-a-Secure-DMZ/

Designing a DMZ (n.d.). SANS Institute InfoSec Reading Room. Retrieved from http://www.sans.org/reading_room/whitepapers/firewalls/designing-dmz_950

Eavesdropping Devices (n.d.). In eavesdropping video online. Retrieved from http://www.tscmvideo.com/eavesdropping/eavesdropping-device.html

Manky D. (2010). Top 10 Vulnerabilities Inside the Network. Retrieved from http://www.networkworld.com/news/tech/2010/110810-network-vulnerabilities.html?page=1

Kim D. & Solomon M.G. (2012). Fundamentals of Information Systems Security. Chapter 3: Malicious Attacks, Threats and Vulnerabilities, 81-116.

Identifying Potential Malicious Attacks, Threats, and Vulnerabilities

IT for Decision Makers
NETWORKING AND SECURITY ISSUES
Handout 1 Overview
Introduction

Many organizations have invested vast amount of money in computer networks, only to find out that although it is providing means of improving the efficiency and productivity of the organization but it also exposes the Organization to possible attacks and threats. Such attacks have been the most challenging issue for most network administrators and a worrying topic for administrators.

Organizations need to share services resources and information but they still need to protect these from people who should not have access to them, while at the same time making those resources available to authorized users. Effective security achieves these goals.

The greatest threat to computer systems and their information comes from humans, through actions that are either malicious or ignorant. When the action is malicious, some motivation or goal is generally behind the attack. For instance, the goal could be to disrupt normal business operations, thereby denying data availability and production.

April 13, 2000, 3:55 P.M. Pacific time: The Web site for the Motion Pictures Association of America (MPAA) is suffering intermittent outages, and the organization suspects computer vandals are to blame. A source inside the organization, who asked not to be identified, said that the MPAA is currently “experiencing problems with their public Web site, and they suspect a denial-of-service attack.” The attack was first rumored on http://www.hackernews.com/, a Web site for news on computer hacking.

Most of the attacks are becoming more frequent and more damaging, and they are using well-known techniques and methods to exploit vulnerability in security policies and systems.

1. Network system.

Before we move to the security part, lets take a few minutes on what a Network system is;

The most popular term - LAN or Local Area Network is a computer network (or data communications network) which is confined to a room, a building, or a group of adjacent buildings. A similar network on a larger scale is sometimes referred to as a WAN (Wide Area Network), or in some cases more specifically, a MAN (Metropolitan Area Network) if it is confined to a single metropolitan area.

The term LAN is most often used to refer to networks created out of a certain class of networking equipment which is tailored to communication over a short distance. This is in contrast to networks, which happen to span short distances, yet are constructed using "WAN" equipment (i.e., equipment capable of transmitting long distances). LAN-style networking equipment typically transmits data at a higher rate than WAN-style equipment: the equipment's design takes advantage of the short distance to supply a high transmission-rate at a relatively low cost.

If you are familiar with network access using a modem and ordinary telephone line, note that both LAN and WAN equipment typically offers faster data transfer than even the fastest ordinary modem/phone-line access, LAN transfers being on the order of a million times faster. This means graphics that are loaded through the network can be displayed significantly faster, and that there are things that it is practical to do on a LAN that you would never do with a modem: for example, you might set up your computer to load your word processing application through the LAN rather than from hard disk; the time you have to wait while it loads would be similar (a few seconds) in either case. In contrast, loading such an application through a modem would require minutes or hours.

A typical use of a LAN is to tie together personal computers in an office in such a way that they can all use a single printer and a file server (briefly, a file server is a computer set up so that other computers can access its hard disk as if it were their own). LANs are also used to transmit e-mail between personal computers in an office, or to attach all the personal computers in the office to a WAN or to the Internet.

There is some variation in the way the term LAN is used:

It is used to refer to a file server and printer, and often the personal computers that are tied to them. People refer to saving their files on the LAN, or on the PC LAN.

It is used more specifically to refer to the data communications wiring and equipment that ties the personal computers to the file server and the printer.

One of the terms associated with most Networks is Ethernet, the most common type in use today. Ethernet is an example of what is called a LAN technology, or in the more specific sense of the word LAN, one of several types of LANs. Some other types of LANs are Token Ring, FDDI, and Fast Ethernet.

What is the Internet?

The Internet is the world's largest network of networks . When you want to access the resources offered by the Internet, you don't really connect to the Internet; you connect to a network that is eventually connected to the Internet backbone, a network of extremely fast (and incredibly

overloaded!) networks components. This is an important point: the Internet is a network of networks -- not a network of hosts.
Services provided by the Internet:
Main services: Electronic mail, File Transfer and Web Browsing.
Defining Security
Computer security is about protecting information. Lately it includes privacy, confidentiality, and integrity.
Some Examples:
- Chinese Foreign Ministry spokesman Zhu Bangzao rejected allegations that China stole U.S. nuclear secrets, saying such claims are meant to undermine China-U.S. relations. Meanwhile, a CIA-led task force was assessing how much damage may have been done to U.S. national security after a Chinese scientist at the Los Alamos National Laboratory in New Mexico allegedly shared nuclear secrets.
March 9, 1999. “CIA measures damage following leaked nuclear secrets.”
http://cnn.com/US/9903/09/china.spy.02/
- Two parties agree and seal their transaction using digital signatures. The signature cannot be ruled invalid by state legislature or other law-making bodies because it uniquely identifies the individuals involved.
October 18, 1999. WASHINGTON (IDG)—The U.S. House Judiciary Committee has approved a bill designed to encourage electronic commerce by recognizing digital signatures as having the same legally binding status as a handwritten signature.
- You visit a Web site and the site collects more personal information than you are willing to divulge or the site distributes data to outside parties. By doing this, it compromises your privacy and opens your world to other parties.
The World Wide Web Consortium (W3C) is developing the Platform for Privacy Preferences Project (P3P)
We need to know the value of the information as defined above in order to develop protective measures that will protect the information from the outside world, while allowing known individuals with unique identities the access required. Here are some protective measures to consider:
Prevention:
Take measures that prevent your information from being damaged, altered, or stolen. Preventive measures can range from locking the server room door to setting up high-level security policies.
Detection:
Take measures that allow you to detect when information has been damaged, altered, or stolen, how it has been damaged, altered, or stolen, and who has caused the damage. Various tools are available to help detect intrusions, damage or alterations, and viruses.
Reaction:
Take measures that allow recovery of information, even if information is lost or damaged.
The above measures are all very well, but if we do not understand how information may be compromised, we cannot take measures to protect it. Here are some components that we can examine on how information can be compromised:
Confidentiality:
The prevention of unauthorized disclosure of information. This can be the result of poor security measures or information leaks by personnel. An example of poor security measures would be to allow anonymous access to sensitive information.
Integrity:
The prevention of erroneous modification of information. Authorized users are probably the biggest cause of errors and omissions and the alteration of data. Storing incorrect data within the

system can be as bad as losing data. Malicious attackers also can modify, delete, or corrupt information that is vital to the correct operation of business functions.

Availability:

The prevention of unauthorized withholding of information or resources. This does not apply just to personnel withholding information. Information should be as freely available as possible to authorized users.

Authentication:

The process of verifying that users are who they claim to be when logging onto a system. Generally, the use of user names and passwords accomplishes this. More sophisticated is the use of smart cards and retina scanning. The process of authentication does not grant the user access rights to resources—this is achieved through the authorization process.

Authorization:

The process of allowing only authorized users access to sensitive information. An authorization process uses the appropriate security authority to determine whether a user should have access to resources.

The Need for Security

Administrators normally find that putting together a security policy that restricts both users and attacks is time consuming and costly. Users also become disgruntled at the heavy security policies making their work difficult for no discernable reason, causing bad politics within the company. Planning an audit policy on huge networks takes up both server resources and time, and often administrators take no note of the audited events. A common attitude among users is that if no secret work is being performed, why bother implementing security.

There is a price to pay when a half-hearted security plan is put into action. It can result in unexpected disaster. A password policy that allows users to use blank or weak passwords is a hacker’s paradise. No firewall or proxy protection between the organization’s private local area network (LAN) and the public Internet makes the company a target for cybercrime.

Organizations will need to determine the price they are willing to pay in order to protect data and other assets. This cost must be weighed against the costs of losing information and hardware and disrupting services. The idea is to find the correct balance. If the data needs minimal protection and the loss of that data is not going to cost the company, then the cost of protecting that data will be less. If the data is sensitive and needs maximum protection, then the opposite is normally true.

Security Threats

Introduction

The first part of this section outlines security threats and briefly describes the methods, tools, and techniques that intruders use to exploit vulnerabilities in systems to achieve their goals.

Security Threats, Attacks, and Vulnerabilities

Information is the key asset in most organizations. Companies gain a competitive advantage by knowing how to use that information. The threat comes from others who would like to acquire the information or limit business opportunities by interfering with normal business processes.

The object of security is to protect valuable or sensitive organizational information while making it readily available. Attackers trying to harm a system or disrupt normal business operations exploit vulnerabilities by using various techniques, methods, and tools.

Attackers generally have motives or goals—for example, to disrupt normal business operations or steal information. To achieve these motives or goals, they use various methods, tools, and techniques to exploit vulnerabilities in a computer system or security policy and controls.

Goal + Method + Vulnerabilities = Attack

Security Threats

Threats can originate from two primary sources: humans and nature. Human threats subsequently can be broken into two categories: malicious and non-malicious. The non-malicious “attacks”

usually come from users and employees who are not trained on computers or are not aware of various computer security threats. Malicious attacks usually come from non-employees or disgruntled employees who have a specific goal or objective to achieve.

Figure 1 introduces a layout that can be used to break up security threats into different areas.
[pic]
Figure 1

Natural Disasters
Nobody can stop nature from taking its course. Earthquakes, hurricanes, floods, lightning, and fire can cause severe damage to computer systems. Information can be lost, system downtime or loss of productivity can occur, and damage to hardware can disrupt other essential services. Few safeguards can be implemented against natural disasters. The best approach is to have disaster recovery plans and contingency plans in place. Other threats such as riots, wars, and terrorist attacks could be included here. Although they are human-caused threats, they are classified as disastrous.

Human Threats
Malicious threats consist of inside attacks by disgruntled or malicious employees and outside attacks by non-employees just looking to harm and disrupt an organization.

The most dangerous attackers are usually insiders (or former insiders), because they know many of the codes and security measures that are already in place. Insiders are likely to have specific goals and objectives, and have legitimate access to the system. Employees are the people most familiar with the organization's computers and applications, and they are most likely to know what actions might cause the most damage.

The insider attack can affect all components of computer security. By browsing through a system, confidential information could be revealed. Insider attacks can affect availability by overloading the system's processing or storage capacity, or by causing the system to crash. People often refer to these individuals as "crackers" or "hackers." The definition of "hacker" has changed over the years. A hacker was once thought of as any individual who enjoyed getting the most out of the system he or she was using. A hacker would use a system extensively and study it until he or she became proficient in all its nuances. This individual was respected as a source of information for local computer users, someone referred to as a "guru" or "wizard."
Now, however, the term hacker refers to people who either break in to systems for which they have no authorization or intentionally overstep their bounds on systems for which they do not have legitimate access.

The correct term to use for someone who breaks in to systems is a "cracker." Common methods for gaining access to a system include password cracking, exploiting known security weaknesses, network spoofing, and social engineering.

Malicious attackers normally will have a specific goal, objective, or motive for an attack on a system. These goals could be to disrupt services and the continuity of business operations by using denial-of-service (DoS) attack tools. They might also want to steal information or even steal hardware such as laptop computers. Hackers can sell information that can be useful to competitors.

In 1996, a laptop computer was stolen from an employee of Visa International that contained 314,000 credit card accounts. The total cost to Visa for just canceling the numbers and replacing the cards was $6 million.

SecurTek Corporation, http://www.securtekcorporation.com/Protect1.ht
Attackers are not the only ones who can harm an organization. The primary threat to data integrity comes from authorized users who are not aware of the actions they are performing. Errors and omissions can cause valuable data to be lost, damaged, or altered.
Non-malicious threats usually come from employees who are untrained in computers and are unaware of security threats and vulnerabilities.
[pic]
Figure 2
The following table gives some examples of the various aspects discussed above.

Threats	Motives/Goals	Methods	Security Policies
• Employees	• Deny services	• Social engineering	• Vulnerabilities
• Malicious	• Steal information	• Viruses, Trojan horses, worms	• Assets
• Ignorant	• Alter information	• Packet replay	• Information and data
• Non-employees	• Damage information	• Packet modification	• Productivity
• Outside attackers	• Delete information	• IP spoofing	• Hardware
• Natural disasters	• Make a joke	• Mail bombing	• Personnel
• Floods	• Show off	• Various hacking tools	
• Earthquakes		• Password cracking	
• Hurricanes			
• Riots and wars			

Note that ignorant employees usually have no motives and goals for causing damage. The damage is accidental. Also, malicious attackers can deceive ignorant employees by using “social engineering” to gain entry. The attacker could masquerade as an administrator and ask for passwords and user names. Employees who are not well trained and are not security aware can fall for this.
Common examples of computer-related employee sabotage include:
• Changing data
• Deleting data
• Destroying data or programs with logic bombs
• Crashing systems
• Holding data hostage
• Destroying hardware or facilities
• Entering data incorrectly
Motives, Goals, and Objectives of Malicious Attackers
There is a strong overlap between physical security and data privacy and integrity. Indeed, the goal of some attacks is not the physical destruction of the computer system but the penetration and removal or copying of sensitive information. Attackers want to achieve these goals either for personal satisfaction or for a reward.
Here are some methods that attackers use:
• Deleting and altering information. Malicious attackers who delete or alter information normally do this to prove a point or take revenge for something that has happened to them. Inside attackers normally do this to spite the organization because they are disgruntled about something. Outside attackers might want to do this to prove that they can get in to the system or for the fun of it.
April 27, 2000: Cheng Tsz-chung, 22, was put behind bars last night after changing the password on

another user’s account and then demanding $500 (Hong Kong currency) to change it back. The victim paid
the money and then contacted police. Cheng has pleaded guilty to one charge of unauthorized access of a
computer and two counts of theft. The magistrate remanded Cheng in custody and said his sentence, which
will be handed down on May 10 pending reports, must have a deterrent effect. Cheng’s lawyer told
Magistrate Ian Candy that his client committed the offenses “just for fun.”

• Committing information theft and fraud. 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. Other targets are systems that control access to any resources, such as time and attendance systems, inventory systems, school grading systems, or long-distance telephone systems
.

• Disrupting normal business operations. Attackers may want to disrupt normal business operations. In any circumstance like this, the attacker has a specific goal to achieve. Attackers use various methods for denial-of-service attacks; the section on methods, tools, and techniques will discuss these.

Methods, Tools, and Techniques for Attacks

Attacks = motive + method + vulnerability. The method in this formula exploits the organization’s vulnerability in order to launch an attack as shown in Figure 2. Malicious attackers can gain access or deny services in numerous ways. Here are some of them:

• Viruses. Attackers can develop harmful code known as viruses. Using hacking techniques, they can break into systems and plant viruses. Viruses in general are a threat to any environment. They come in different forms and although not always malicious, they always take up time. Viruses can also be spread via e-mail and disks.

• Trojan horses. These are malicious programs or software code hidden inside what looks like a normal program. When a user runs the normal program, the hidden code runs as well. It can then start deleting files and causing other damage to the computer. Trojan horses are normally spread by e-mail attachments. The Melissa virus that caused denial-of-service attacks throughout the world in 1999 was a type of Trojan horse.

• Worms. These are programs that run independently and travel from computer to computer across network connections. Worms may have portions of themselves running on many different computers. Worms do not change other programs, although they may carry other code that does.

• Password cracking. This is a technique attackers use to surreptitiously gain system access through another user’s account. This is possible because users often select weak passwords. The two major problems with passwords is when they are easy to guess based on knowledge of the user (for example, wife’s maiden name) and when they are susceptible to dictionary attacks (that is, using a dictionary as the source of guesses).

• Denial-of-service attacks. This attack exploits the need to have a service available. It is a growing trend on the Internet because Web sites in general are open doors ready for abuse. People can easily flood the Web server with communication in order to keep it busy. Therefore, companies connected to the Internet should prepare for (DoS) attacks. They also are difficult to trace and allow other types of attacks to be subdued.

• E-mail hacking. Electronic mail is one of the most popular features of the Internet. With access to Internet e-mail, someone can potentially correspond with any one of millions of people worldwide. Some of the threats associated with e-mail are:

Impersonation. The sender address on Internet e-mail cannot be trusted because the sender can create a false return address. Someone could have modified the header in transit, or the sender could have connected directly to the Simple Mail Transfer Protocol (SMTP – the protocol used for sending e-mail) port on the target computer to enter the e-mail.
Eavesdropping. E-mail headers and contents are transmitted in the clear text if no encryption is used. As a result, the contents of a message can be read or altered in transit. The header can be modified to hide or change the sender, or to redirect the message.

• Eavesdropping. This allows a cracker (hacker) to make a complete copy of network activity. As a result, a cracker can obtain sensitive information such as passwords, data, and procedures for performing functions. It is possible for a cracker to eavesdrop by wiretapping, using radio, or using auxiliary ports on terminals. It is also possible to eavesdrop using software that monitors packets sent over the network. In most cases, it is difficult to detect eavesdropping.

• Social engineering. This is a common form of cracking. It can be used by outsiders and by people within an organization. Social engineering is a hacker term for tricking people into revealing their password or some form of security information.
• Intrusion attacks. In these attacks, a hacker uses various hacking tools to gain access to systems. These can range from password-cracking tools to protocol hacking and manipulation tools. Intrusion detection tools often can help to detect changes and variants that take place within systems and networks.
Note: Additional handout on viruses.
Security Vulnerabilities
As explained previously, a malicious attacker uses a method to exploit vulnerabilities in order to achieve a goal. Vulnerabilities are weak points or loopholes in security that an attacker exploits in order to gain access to the network or to resources on the network (see Figure 2). Remember that the vulnerability is not the attack, but rather the weak point that is exploited. Here are some of the weak points:
• Passwords. Password selection will be a contentious point as long as users have to select one. The problem usually is remembering the correct password from among the multitude of passwords a user needs to remember. Users end up selecting commonly used passwords because they are easy to remember. Anything from birthdays to the names of loved ones. This is vulnerability because it gives others a good chance to guess the correct password.
• Protocol design. Communication protocols sometimes have weak points. Attackers use these to gain information and eventually gain access to systems.
• Modems. Modems have become standard features on many desktop computers. Any unauthorized modem is a serious security concern. People use them not just to connect to the Internet, but also to connect to their office so they can work from home. The problem is that a modem is a means of bypassing the “firewall” that protects a network from outside intruders. A hacker using a “war dialer” tool to identify the modem telephone number and a “password cracker” tool to break a weak password can gain access to the system. Due to the nature of computer networking, once a hacker connects to that one computer, the hacker can often connect to any other computer in the network.
Some Examples:
Example 1: non-malicious threat (ignorant employees).

An employee known here as John Doe copies games and other executables from a 1.44 MB disk onto his
local hard drive and then runs the executables. Unfortunately, the games contained various viruses and
Trojan horses. The organization had not yet deployed any anti-virus software. After a short time, John Doe
and other employees began to notice strange and unforeseen events occurring on their computers, causing
disruption of services and possible corruption of data. The following figure explains the various vulnerabilities that existed and the loss in assets that are involved.
[pic]
Figure 3
Example 2: malicious threat (malicious attackers)
An employee known here as Sally was turned down for promotion three times. Sally believes that she has
put in a considerable amount of work and overtime and is being turned down for promotion because she is
too young. Sally has a degree in computer science and decides to resign from the company and take
revenge on it by causing the company's Web server to stop servicing requests. Sally uses a denial-of
service attack tool called Trin00 to start an attack on the company's Web server.
Most of the company's business is conducted via e-commerce and clients are complaining that they cannot
connect to the Web server. The following diagram outlines the various tools and vulnerabilities Sally used to
achieve her goal.
[pic]
Figure 4
Example 3: natural disasters
An organization has various modems and Integrated Services Digital Network (ISDN) router installations and does not have surge protection. During a thunderstorm, lightning strikes the telephone and ISDN lines. All modems and ISDN routers are destroyed, taking with them a couple of motherboards. The following diagram shows the vulnerability and the loss of assets.
[pic]
Figure 5
Security Policies and plans.
Security Policies are the foundation, the bottom line of information security of an organization. Each organization would present a different policy plan that is appropriate, clear and effective for the organization.
Design and implement a security plan.
Designing a security plan includes setting security goals and strategies and deciding on the level of security that is appropriate. Deciding on the level of security means weighing the pros and cons of higher versus lower security. Higher security requires more administration but ensures only the right people will have access to your resources. Lower security creates a more flexible and open environment, but might not be as secure as other configurations.
Understand and implement security policy.
Security policy enforces uniform security standards for groups of users. Security policy is used to establish a basis of security for the environment. Different from user rights and permissions, security policy applies to all users or objects in the deployment.

Planning for Security.

Although security technologies are highly advanced, effective security must combine technology with good planning for business and social practices. No matter how advanced and well implemented the technology is, it is only as good as the methods used in employing and managing it.

Implementing the appropriate security standards is a key issue for most organizations. To implement security standards, devise a security plan that applies a set of security technologies consistently to protect the organization's resources.

A typical security plan might include the following sections:

• Security goals: Describe what the organization needs protecting.

• Security risks: Enumerate the types of security hazards that affect the enterprise, including what poses the threats and how significant the threats are.

• Security strategies: A description of the general security strategies necessary to meet the threats and mitigate the risks.

• Security group descriptions: Describe security groups and their relationship to one another. This section maps security policies to security groups.

• Security Policy: Describe Group Policy security settings, such as network password policies.

• Network logon and authentication strategies: In a networked environment, consider authentication strategies for logging on to the network and for using remote access or smart card to log on.

• Information security strategies: How to implement information security solutions, such as an encrypted file system (EFS), Internet Protocol security, and access authorization using permissions.

• Administrative policies: Include policies for delegation of administrative tasks and monitoring of audit logs to detect suspicious activity.

For starters, the easiest way to deal with security policies is to use some pre-written "off the shelf". This is certainly a reasonable approach, but it is important to ensure that the policies are of the requisite standard, and perhaps are compliant with standards.

An example: http://www.securitypolicy.co.uk/secpolicy/

Conclusion

Malicious attackers will use various methods, tools, and techniques to exploit vulnerabilities in security policies and controls to achieve a goal or objective. Non-malicious attacks occur due to poor security policies and controls that allow vulnerabilities and errors to take place. Natural disasters can occur at any time, so organizations should implement measures to try to prevent the damage they can cause.

Some Online Publications

Bagwill, Robert, and Barbara Guttman. Internet Security Policy: A Technical Guide. National Institute of Standards and Technology Computer Security Division.
http://csrc.nist.gov/isptg/html/

Bassham, Lawrence E., and W. Timothy Polk. Threat Assessment of Malicious Code and Human Threats. National Institute of Standards and Technology Computer Security Division.
http://csrc.nist.gov/nistir/threats/

Bort, Julie. A False Sense of Security. Lantimes.
http://www.lantimes.com/98/98jul/807b023a.html

Brown, Carol E. and Alan Sangster. Electronic Sabotage.
http://www.bus.orst.edu/faculty/brownc/lectures/virus/virus.htm

Chess, David. Things that Go Bump in the Net.
http://www.research.ibm.com/massive/bump.html/

Huegen, Craig. Network-Based Denial of Service Attack Information.
http://users.quadrunner.com/chuegen/smurf/

Martin, Brian. Have Script Will Destroy (Lessons in DoS). http://www.attrition.org/
Null, Christopher. Is the Hacker Threat Real? Lantimes.
http://www.lantimes.com/98/98mar/803b007a.html
Parker, Donn. Automated Crime. http://www.infosecuritymag.com/
DDOS Debriefing. http://www.infosecuritymag.com/
Department of Defense Trusted Computer System Evaluation Criteria (Orange Book). National Computer Security Center. http://csrc.ncsl.nist.gov/secpubs/rainbow/std001.txt
Trusted Network Interpretation (Red Book). National Computer Security Center.
http://csrc.ncsl.nist.gov/secpubs/rainbow/tg005.txt
Web Sites
For more information on viruses, Trojan horses, and Internet hoaxes, see:
• The Computer Incident Advisory Capability site at http://ciac.llnl.gov
• The E-Commerce Webopedia at http://e-comm.webopedia.com/
• http://www.cert.org
• http://www.blueroom.com/internet/
For more information on distributed denial-of-service attacks, see http://www.icsa.net/
For more information on back-end system issues for online financial sites, see
http://www.incurrent.com/
For more information about security, see the Pretty Good Privacy site at http://www.pgp.com.
Additional sites on security issues:
http://www.nwfusion.com/
http://www.interhack.net/
http://www.nai.com/
http://www.cert.org/
http://www.antionline.com/
http://www.infosyssec.com/