Insider Threats

The following describes general insider threats.

System Users

Unauthorized access includes all incidents where an authorized user, either accidentally or deliberately, bypasses access controls and accesses information which results in the IT assets being disclosed, modified, or destroyed. User error in all organizations presents the greatest single risk to the compromise of information and systems. Choosing weak passwords, recording them in an insecure manner, and sharing passwords represent a significant vulnerability. Improper configuration, or changing the configuration of the workstation to enable greater sharing of information without authorization, can expose sensitive information to unauthorized access.

Attaching a sensitive document to e-mail without encrypting the document risks having the document read by someone other than the intended recipient. Without encryption, and digital signatures, there is no guarantee that the message has not been tampered with during transmission, or that only authorized persons have had access to the message. This represents a significant risk to the confidentiality and integrity of any sensitive information that traverses the network. Users can compromise privacy, where information is disclosed to unauthorized individuals, by attaching the wrong file to an e-mail, by improper sharing of files, or by inadequately protecting data on the workstation and the network. Lack of user awareness may result in a user transfer of large files that exceed the network capacity, with a resultant loss of availability of the network service.

Copyright Violations

Workstation and server software protected by copyright laws may be copied for personal use. With no control on media entering or leaving the premises, this activity could expose an organization to legal action, as well as public embarrassment, should it occur.

Contractors, Visitors, Office Cleaning Personnel

Unauthorized access includes all incidents where legitimate contractors, visitors, or cleaning personnel access information, which results in the information being disclosed, modified or destroyed.

Compromising Emanation Attack

It is a well-known fact that electronic devices produce electromagnetic fields, which can cause interference to radio and television reception. These signals can be picked up with monitoring devices that are relatively inexpensive to buy, or build, and do not require a great deal of sophisticated knowledge to operate. It is the exploitation of this phenomenon that constitutes a compromising emanation attack.

Data Entry Errors

Entering erroneous data into a system, file, database or other data repository by accident. Data entry errors are more likely to occur when users are untrained, overworked, stressed, disgruntled or otherwise impaired.

Disgruntled Employee

Any employee who becomes disgruntled can become a threat quite easily. This could result in an individual attempting to delete files, disclosing sensitive data to unauthorized persons, disrupting communications, vandalizing equipment, or even physically harming personnel. Changes in infrastructure and outsourcing beyond the control of the organization can have a negative impact on employee attitude, especially if they feel their job is at stake.

Electronic Eavesdropping

This attack is similar in nature to the emanation attack in that clandestine monitoring devices intercept the signals emanating from the target device or system. The main difference is in the location of the monitoring device. Eavesdropping can be accomplished without any physical connection to the system, but more frequently involves actually connecting to the system (i.e. using network sniffers, wiretaps or bugs).

Equipment Malfunction

Hardware equipment can fail at any time, which can threaten the confidentiality, integrity or availability of services or data. A failed hard disk drive may render the data unrecoverable or a failed web server may disrupt services.

Exploitation of Unattended Open Sessions

Unauthorized persons accessing workstations, servers, networks, etc., which have been logged on by legitimate users, left unattended with no time-out feature active or time-out feature excessive in length. Once the unauthorized individual has gained access to the system, they can compromise data, processes and other system resources with the privileges gained from the hijacked open session.

Human Errors

Inadvertent errors or omissions by users could cause unauthorized disclosure, destruction, removal, modification or interruption of sensitive information, assets or services. Human error is generally considered to be one of the major threats to IT systems and networks.

Illness, Injury or Death

The temporary or permanent loss of key personnel due to illness, injury or death can affect the availability of services. If only one person is knowledgeable or permitted to perform this task and is not available, it may be difficult to continue operations until the individual returns to work.

Loss of Equipment or Media

Loss of equipment such as laptop computers, loss of media such as floppy disks or CD-ROMS, and loss of paper documentation can affect the availability of services or confidentiality of data.

Negligence or Misuse

Personnel who are negligent in their duties or who misuse system resources, may affect the confidentiality, integrity or availability of systems or data in the system. For example, users may install games or other unauthorized software.

Software Malfunction

There is always a possibility of a software application failing due to programming or software bugs or errors, which can affect the confidentiality, integrity or availability of system services or data. A faulty encryption algorithm or file deletion utility can leave sensitive data exposed, other faults may corrupt data, while still others may render data unreadable.

Theft of Information

The illegal removal of information from a system, either by physical means (stealing computer storage media), or by electronic means (making illegal copies of sensitive data), compromises the confidentiality of data. In the case of actually stealing storage media, availability may also be affected, if no other copies of the information are available.

Theft of System and Hardware Components

Many computer and communications devices and components are attractive to thieves who may be removing items for resale or personnel use. Incidents of theft of computer memory, hard drives, video cards and other components have led many organizations to install protective security screws and lock-down cables on essential and attractive items to reduce the likelihood of theft. Theft of components can affect the integrity, availability and confidentiality of data and resources.

Unauthorized Access to System/Data by Person With Access Privileges

This threat consists of an individual with access privileges on the system attempting to access data and resources that he/she does not have privileges to access. It may consist of a user for example trying to gain administrator privileges to make changes to the system configuration, install unauthorized software or perform other tasks.

Unauthorized Access to System/Data by Person Without Access Privileges

This threat consists of an individual who does not have access privileges to the system and attempting to access the system data and resources. It may consist of a cleaner working on the night shift trying to gain access to a computer terminal for a variety of reasons. This attack requires the threat agent to have physical access to the target wherein he/she is attempting to gain logical access to the target.

Labour Relations/Strike

Labour relations, disputes and actions such as strikes can impact the availability of functions and systems. This increases the likelihood of malicious action by authorized internal users with the intention of disrupting the availability or integrity of the network, including both software and hardware assets.

External Threats

The following describes general external threats.

Malicious Code

The term malicious code encompasses a variety of potential threats that can place a system or network at risk. A description of some of the more common threats are covered below:

A virus can affect a system or data within a system in many ways and can be quite unpredictable in nature. They usually affect the confidentiality, integrity or availability of the data, but they can even affect the integrity and availability of systems themselves. A virus incident can lead to excessive usage of resources whether it's bandwidth, personnel or storage space on workstations and servers.

A Trojan horse is an apparently useful program containing hidden functions that can exploit the privileges of the user [running the program], with a resulting security threat. A Trojan horse does things that the program user did not intend. Trojan horses rely on users to install them. Intruders, who have gained unauthorized access, can install them. Then, an intruder attempting to subvert a system using a Trojan horse relies on other users running the Trojan horse to be successful.

Trojan horses can do anything that the user executing the program has the privileges to do. This includes:

- deleting files that the user can delete;
- transmitting to the intruder any files that the user can read;
- changing any files that the user can modify;
- installing other programs with the privileges of the user, such as programs that provide unauthorized network access;
- executing privilege-elevation attacks, that is, the Trojan horse can attempt to exploit a vulnerability to increase the level of access beyond that of the user running the Trojan horse. If this is successful, the Trojan horse can operate with the increased privileges;
- installing viruses; and
- installing other Trojan horses.

A compromise of any system on a network, including a compromise through Trojan horses, may have consequences for the other systems on the network. Particularly vulnerable are systems that transmit authentication data, such as passwords over shared networks, in clear text. If a system on the network is compromised via a Trojan Horse or another method, the intruder may be able to install a network sniffer and record usernames and passwords or other sensitive information as it traverses the network

Hacking

IT assets are subject to hacking attacks by individuals or organizations such as amateur or professional hackers, criminals or special interest groups. Hackers may disrupt system availability by making configuration changes, introducing errors into system routines or by overwriting essential files with unwanted data. They could do this as a malicious attack or just through negligence, mistakes or ineptness. As well, they could deliberately introduce viruses or other malicious code onto a system for the purpose of disrupting services, modifying system processes or data, or gathering information.

Hacktivism
The union of hacking and activism; for example, operations that use hacking techniques against a target's internet site with the intent of disrupting normal operations but not causing serious damage. 'Web sit-ins' and virtual blockades, automated email bombs, web hacks, computer break-ins, and computer viruses and worms are all examples of hacktivism.

Cyberterrorism
The convergence of cyberspace and terrorist activity; for example, politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage. Concerns that terrorist groups or individuals may penetrate a nation's electronic energy, transportation, financial or security grid or system and cause catastrophic damage (nuclear reactor or dam failure, multiple mid-air collisions or downed airliners, disrupting national economies through stock market interference, etc.) are all related to the phenomenon known as cyberterroris

Default Password Attacks

Many computer systems come from the manufacturer with default passwords set. Computer hackers and other groups commonly know these passwords. It is quite common for busy system administrators to fail to change these passwords, thereby leaving their systems open to attack by these individuals. A hacker will often try, as a first step, to infiltrate the management functions, or utilities of a router, switch or other device by entering the default password.

Human Errors

Inadvertent errors or omissions by individuals external to the controlled mission environment that could cause unauthorized disclosure, destruction, removal, modification or interruption of sensitive information, assets or services.

Masquerade

A masquerade attack involves an individual, application or system impersonating another individual, application or system in an attempt to receive services or data that would normally be provided to the target, but not to the attacker. An example of this type of attack could involve a malicious program sitting on a server or workstation waiting for a user to log in. The malicious program masquerades as the legitimate login program and asks for the user identification and password. Once the user enters the data, the malicious program stores the information and feeds the login info to the legitimate program. It then passes the user back to the legitimate program and terminates. Depending on how the rogue program operates, it may forward the user id/password data to another location or store it locally for the attacker to retrieve at an opportune time. Strict auditing combined with layered defensive systems will help determine if traffic flows match this pattern.

Spoofing

In a spoofing attack, the agent is attempting to make the target user, system or process believe that the data they received is legitimate when, in fact, it has been altered in some form. For example, an unauthorized person could attempt to impersonate a client by entering his name and address on the web form.

General Subversion

Deliberate acts or omissions by external threat agents that are intended to undermine employee morale, management resolve or public confidence.

Industrial Espionage

This involves collecting proprietary data from private corporations or government agencies for the benefit of another company or organization. Industrial espionage can be perpetrated either by companies seeking to improve their competitive advantage or by governments seeking to aid their domestic industries.

Economic Espionage
This can be described as illegal, clandestine or coercive activity by a foreign government in order to gain unauthorized access to economic intelligence, such as proprietary information or technology, for economic advantage.

Criminal Activity
A general threat that involves any illegal in the context of exploitation of IT assets.

Vandalism

The deliberate modification, interruption or destruction of computer and communications systems, processes or data with no political, religious, ideological or other motive except for personal gratification. The targets of vandalism can be directed or random in nature. Any system connected to the Internet is a potential target for vandals.

Environmental Threats and Acts of Nature

The following describes general environmental threats.

Power Failure

Power outage caused by an accidental or destructive act of nature can interrupt availability of computer systems.

Water Damage

Sprinkler leaks from fire prevention systems can have catastrophic consequences for the availability of computer systems.

Fire

The occurrence of an accidental or deliberate fire can cause serious interruption to the service.

Natural Disasters

Any act of nature that could cause unauthorized disclosure, destruction, removal, modification or interruption of sensitive information, assets or services, or injury to people. Natural disasters can cause any number of serious after-effects, which could include events such as fires, gas-line ruptures, building collapses, injury and death. Severe weather events such as tornadoes and hurricanes can affect the availability of IT systems, if transmission lines and other communications devices are broken, buildings are destroyed or personnel injured. Examples of natural disasters include excessive heat/cold, wind, lightning, freezing rain, snow, hail, tornadoes, hurricanes, earthquakes and landslides.