Threats and Vulnerabilities

Proficiency Code: A

Hostile information operations/information cyber-warfare activities pose the greatest threats to an organization's mission critical information via its CISs. Use of commercial hardware and software, in combination with extensive network connectivity, provides many potential avenues for information operations/information cyber-warfare attacks. Such attacks, including introduction of malicious codes (malware), trap doors, or viruses, could result in disabling operations, unauthorized monitoring, and denial or manipulation of communications and information. Various techniques can jam or spoof communications or otherwise degrade or deny access to CISs. Additionally, CISs are vulnerable to espionage and sabotage (especially from individuals who have legitimate access to the system or the physical plant in which it is housed), and to physical damage or destruction. Further, Telecommunications Electronic Material Protected From Emanating Spurious Transmissions (TEMPEST) hazards (compromising emanations or unintentional signals) that, if intercepted and analyzed, would disclose the information transferred, received, handle, or otherwise processed by an information-processing system.

Secure national security systems are vitally important to the operational effectiveness of the warfighter. The Air Force COMSEC program meets Public Law, National, and DOD requirements to secure or protect classified and sensitive information processed using Air Force information systems.

Vulnerability is a problem, or weakness, in a computer system that allows an intruder or hacker to exploit the system's information security. Vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw.

Computer Security and Information Assurance Threats and vulnerabilities

It is unlikely that we can ever achieve total IS security even with the controls and safeguards we have in place. New threats and vulnerabilities continue to emerge so the Air Force is always working to identify and analyze them so we can maintain an appropriate level of protection through established safeguards based on security requirements. Headquarters Air Force Communication Agency (HQ AFCA) and the program manager develop and coordinate the schedules and details for network assessment. The particular details of network risk assessment depend on the system design, environment, and classification of data on that network. COMPUSEC and IA threats cause harm to information (data) or to the IS that process that data. Threats exist from natural, environmental, human, and viruses. We will discuss each one briefly.

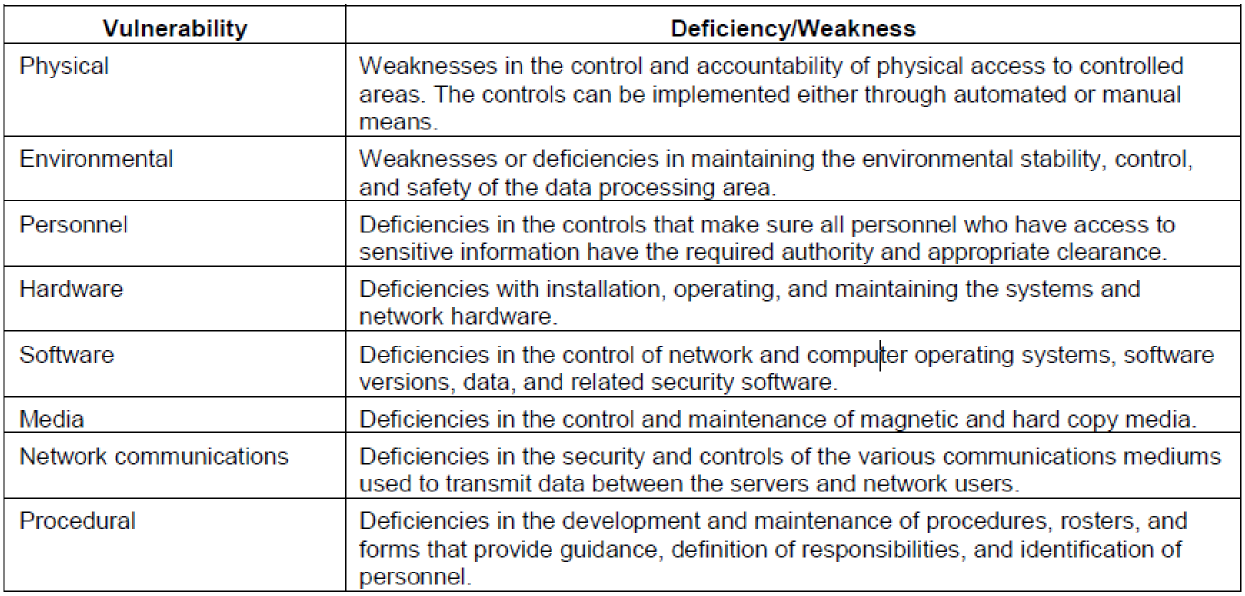
Nature causes natural threats, which includes earthquakes, floods, hurricanes, snow/ice, tornado/windstorms, lightning, or severe storms. Every location is subject to some of these types of threats and therefore must have precautionary measures to minimize system damages.
Environmental

Environmental threats result from man-made items in the environment. These can include flaws in building construction, improper implementation of utilities, inadequate wiring and poor housekeeping practices. Program managers along with the facility management should work together to identify environmental inadequacies.

Human threats can be either intentional or unintentional. Intentional threats are deliberate attacks by an individual to degrade or damage information systems, network resources, or information. Reasons for intentional attacks could include degrading system integrity, revenge, or personal gain. Unintentional threats cause inadvertent damage to ISs due to lack of training, carelessness, or accidental intrusions. A computer system is no more secure than the persons responsible for its operation are. Malicious individuals have regularly penetrated well-designed, secure computer systems by taking advantage of the carelessness of trusted individuals or by deliberately deceiving them.

One of the most common COMPUSEC threats is software viruses. Software viruses are software programs that destroy data on computers that contract them. They also can spread from computer system to computer system. Damages from viruses can result in: reformatting a hard disk; erasing programs and files; adding unrecognizable characters to files; or destroying disk directories and file allocation tables preventing the computer from using the tables or directories to locate files. One of the newest threats comes from spyware. Spyware is computer software that collects personal information about users without their informed consent.

COMPUSEC and IA vulnerabilities are weaknesses in ISs or security procedures that can be exploited by the threats. Vulnerabilities are listed in the table below.



Vulnerability	Deficiency/Weakness
Physical	Weaknesses in the control and accountability of physical access to controlled areas. The controls can be implemented either through automated or manual means.
Environmental	Weaknesses or deficiencies in maintaining the environmental stability, control, and safety of the data processing area.
Personnel	Deficiencies in the controls that make sure all personnel who have access to sensitive information have the required authority and appropriate clearance.
Hardware	Deficiencies with installation, operating, and maintaining the systems and network hardware.
Software	Deficiencies in the control of network and computer operating systems, software versions, data, and related security software.
Media	Deficiencies in the control and maintenance of magnetic and hard copy media.
Network communications	Deficiencies in the security and controls of the various communications mediums used to transmit data between the servers and network users.
Procedural	Deficiencies in the development and maintenance of procedures, rosters, and forms that provide guidance, definition of responsibilities, and identification of personnel.