Vulnerability

It is the weakness in a system, for example in procedure, design or implementation that might be exploited to cause loss or harm. Vulnerabilities in computer systems are; weak authentication, lack of access control, errors in programs, finite or insufficient resources, and inadequate physical protection. When these vulnerabilities are paired with a credible attack of any kind, each of these vulnerabilities can allow harm to confidentiality, integrity, or availability. Vulnerabilities are usually due part of the system and not human of environmental.

Threats

A threat to a computing system is a set of circumstance that has the potential to cause a loss or harm. The types of threats are non-human and human threats. Human threats can be categorize into two; non-malicious or malicious. Malicious attacks can be classified as random or directed. While a threat is an incident that could cause harm, vulnerability is a weakness through which harm could occur. These two problems can combine to cause harm. Also they can cause harm without the other, but a threat exercising vulnerability means damage.

Control

Control is an action, device, procedure or technique that removes or reduces vulnerability, in order to stop harm from happening. Harm occurs when a threat is realized against vulnerability. Control uses these steps to deal with harm; prevent, deter, deflect, mitigate, detect, recover. Thus control work in most situations, by either blocking or diminishing the threat, or close the vulnerability.