Vulnerabilities, Threats, Attacks, and Controls

A computer-based system has three separate but valuable components: hardware, software, and data. Each of these assets offers value to different members of the community affected by the system

Vulnerability

A vulnerability is a weakness in the security system, for example, in procedures, design, or implementation, that might be exploited to cause loss or harm. For instance, a particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access.

Threat

A threat to a computing system is a set of circumstances that has the potential to cause loss or harm. There are many threats to a computer system, including human-initiated and computer-initiated ones. We have all experienced the results of human errors, hardware design flaws, and software failures. But natural disasters are threats, too; they can bring a system down when the computer room is flooded or the data center collapses from an earthquake, for example.

A human who exploits a vulnerability perpetrates an attack on the system. An attack can also be launched by another system, as when one system sends an overwhelming set of messages to another, virtually shutting down the second system's ability to function. Unfortunately, we have seen this type of attack frequently, as denial-of-service attacks flood servers with more messages than they can handle