Lecture cast notes

Title: History and Definitions

Network and Information Security Management encompasses the following areas:

Cybersecurity, Information Security, Computer security and Information assurance

Brief history

Cybersecurity history dates back to 1965 - when we had the CTSS which allowed multiple users to access a central computer system. The field has evolved over time seeing a wide range of cyber threats such as worms, ransomware attacks, botnet attacks, phishing attacks and so on.

Some Key Definitions by ISO/IEC 27000:2012

Threat: "the potential cause of an unwanted incident, which may result in harm to a system or organization."

Vulnerability: "a weakness of an asset or control that can be exploited by one or more threats."

Core concepts of Information Security

The four tenets of information security as defined by **ISO/IEC 27000:2012** are:

Confidentiality:
"Information is not made available or disclosed to unauthorized individuals and entities or processes."-

Integrity: "the property of accuracy and completeness of assets."

Availability: "the property of being accessible and usable upon demand by an authorized entity."

Non-repudiation: "ability to prove the occurrence of a claimed event or action and its originating entities."

Stride and Dread Tool

To support the threat modelling process, Microsoft also created a threat classification known as **Stride**, and a Risk rating system known as **Dread**.

STRIDE
Stride classifies threats into six main categories:

Spoofing: Attacker pretends to be someone else

Tampering: the attacker tries to modify an asset

Repudiation: opposite of non-repudiation

Information Disclosure: The attacker gets unauthorised access to information

Denial of Service: the attacker makes the assets unavailable to users

Elevation of privileges: the attacker raises his level of access to a system

The Dread risk rating defines the risk associated with any given threat, where each element is rated numerically, often out of ten.

DREAD Risk = (Damage + Reproducibility + Exploitability + Affected Users + Discoverability) / 5

Damage: the amount of damage the attack could cause

Reproducibility: how easy it is to reproduce the threat or attack

Exploitability: how easy it is to exploit the threats – does it need special tools or skills?

Affected users: how many people would be affected by the threat?

Discoverability: Is the threat secret or in the public domain?

Common cybersecurity roles

Some common cybersecurity roles are penetration tester, business continuity analyst, information risk analyst and information manager.

Reference

Network and Information Security Management Module (2021) *History and Definitions.* [Lecturecast]. NISM_PCOM7E Network and Information Security Management. University of Essex Online.

ISO/IEC 27000:2012(en).Available from: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-2:v1:en [Accessed 10 August 2021]