Information Security Fundamentals

Course Summary

Description

This course provides students a foundation to understand Information Security, how it affects their organization, and how to critically examine their management of sensitive information and assets.

Objectives

By the end of this course, students will be able to:

- Understand the methods, motivations and abilities of hackers
- Properly construct a flexible and effective security policy
- Understand best practices to secure and protect servers, desktops, applications, and information
- Conduct vulnerability scans and audits of your networks, systems

Topics

- Threat Risk Assessment
- External Risks to Information Security
- Internal Risks to Information Security
- Effective Safeguards to Information

Audience

This course is valuable to anyone who works with corporate, government, or otherwise sensitive information assets.

Prerequisites

There are no prerequisites for this course.

Duration

One day

Information Security Fundamentals

Course Outline

I. Threat Risk Assessment
- A. Definition of Assets
- B. Threat Assessment
- C. Risk Assessment
- D. Recommendations

II. External Risks to Information Security
- A. Social Engineering
- B. Desktop and Network Security
- C. Espionage and Physical Security

III. Internal Risks to Information Security
- A. Blackmail, Fraud, and Bribery
- B. Employee Abuse
- C. Loss of forensic integrity

IV. Effective Safeguards for Information
- A. How to implement new IS policy
- B. Constructing an effective audit plan
- C. The importance of an Incident Response Plan