

2000 to Present

1. Discuss how today, the Internet has brought millions of unsecured computer networks into communication with each other.
2. Explain that our ability to secure each computer's stored information is now influenced by the security on each computer to which it is connected.

What is Security?

1. Explain security in general and point out the Committee on National Security Systems (CNSS) as the protection of information and its critical elements.
2. Discuss how a successful organization should have the following multiple layers of security in place for the protection of its operations:
 - Information security management
 - Data security
 - Network security
3. Discuss the C.I.A. triangle, which has been considered the industry standard for computer security since the development of the mainframe. It was solely based on three characteristics that described the utility of information: confidentiality, integrity, and availability. The C.I.A. triangle has expanded into a list of critical characteristics of information.

CNSS Security Model

1. Discuss the security model. Your primary responsibility is to make sure that each of the 27 cells is properly addressed during the security process.

Approaches to Information Security Implementation

1. Explain that security can begin as a grassroots effort when systems administrators attempt to improve the security of their systems. This is referred to as the bottom-up approach.
2. Discuss the key advantage of the bottom-up approach.
3. Explain an alternative approach, which has a higher probability of success; that is the top-down approach.

Security in the Systems Development Life Cycle

1. Explain the traditional approach for implementing an information security system in an organization. This has given rise to a number of variations, including RAD, JAD, Agile, and a new approach, DevOps.
2. Explain joint application development (JAD) and rapid application development (RAD) approaches.

3. Explain the DevOps approach

The Systems Development Life Cycle

1. Explain the SDLC methodology for the design and implementation of an information system in an organization.

Traditional Development Methods

1. Explain that the traditional SDLC that consists of six phases and is known as the waterfall model.

Software Assurance

1. Define software assurance (SA) as a methodological approach that seeks to build security into the development life cycle rather than address it at later stages.

The NIST Approach to Securing the SDLC

Note that NIST recommends that organizations incorporate the associated IT security steps of the included general SDLC into their development processes. It is imperative that information security be designed into a system from its inception, rather than added in during or after the implementation phase.

1. Point out that organizations are moving toward more security-focused development approaches, seeking to improve not only the functionality of the systems they have in place, but the confidence of the consumer in their product.

Senior Management

1. Explain the Chief Information Officer roles and responsibilities.
2. Explain who is the Chief Information Security Officer

Information Security Project Team

1. Discuss the individuals who comprise the project team and explain that they are experienced in one or multiple facets of the required technical and nontechnical areas.
 - **Champion:**
 - **Team leader:**
 - **Security policy developers:**
 - **Risk assessment specialists:**
 - **Security professionals:**
 - **Systems administrators:**
 - **End users**

Data Responsibilities

1. Discuss and define the roles of those who own and safeguard the data.
 - **Data Owners:**
 - **Data Custodians:**
 - **Data Users:**

Information Technology Management and Professionals

1. Discuss why technology managers often focus on operating the technology operations with a focus on cost and not necessarily on security.

Computer and Information Security

1. What is the primary difference between computer security and information security?

Useful Websites:

1. Internet Society – Histories of the Internet
<http://www.isoc.org/internet/history/brief.shtml>
2. CNSS National Information Assurance Glossary
https://www.ncsc.gov/nittf/docs/CNSSI-4009_National_Information_Assurance.pdf
3. Microsoft Security Development Lifecycle
<http://www.microsoft.com/security/sdl/>
4. The Role of a Chief Security Officer
<http://www.govtech.com/security/The-Role-of-Chief-Security-Officer-is-More-Vital-than-Ever.html>
5. National Training Standard for Information Security Professionals at
<http://www.sait.fsu.edu/resources/NSTISSI-4011.pdf>
6. alternative view of the components of an information system, from the business perspective, refer students to this MBA view at
<http://www.mbaknol.com/management-information-systems/components-of-an-information-system/>