INFORMATION ASSURANCE AND SECURITY

THE DEMAND FOR SECURITY

Theodore Ross Bermejo - Ivern Bryant Buala - Franz Meinard Chang

Lesson 2

INTRODUCTION

- *The core aim of an information security program, unlike any other information technology program, is to ensure that systems and their contents remain the same.*

- *Organizations spend hundreds of thousands of dollars and tens of thousands of work hours to keep their data systems up to date. These resources may be used to improve the systems that support the information if risks to information and systems did not exist.*

- *Attacks on information systems, on the other hand, happen on a regular basis, and the demand for information security rises in tandem with the sophistication of such attacks.*

BUSINESS NEEDS FIRST

For a company, information security serves 4 critical functions:

- *Keeping the company's ability to function safe.*
- *Ensure that applications operating on the organization's IT platforms are safe to use.*
- *Keeping the data that the company obtains and utilizes safe.*
- *Keeping the company's technological assets safe.*

PROTECTING AN ORGANIZATION'S FUNCTIONALITY

Implementing information security to ensure the organization's operational continuity is a shared responsibility between general management and IT management. Despite the perception that information security is a complex technical challenge, it is fundamentally more about management than technology.

Moreover, managing information security focuses primarily on policy formulation and enforcement rather than on the technological tools utilized for its implementation. This comparison is akin to how managing payroll is centered on management practices rather than solely on the calculations involved in wage computation.

According to Charles Cresson Wood, a well-known information security author: In truth, most of information security is effective information technology management. Many individuals believe that adding additional technology to a problem would solve it. Not necessarily... So, out of necessity, I've spent a lot of my time trying to persuade my customers to view information security as a management issue as well as a technical issue, and information security as a people issue as well as a technical issue.

Rather than isolating security as a technical concern, each of an organization's communities of interest must address information security in terms of commercial effect and the cost of business interruption.

PROVIDING A SAFE ENVIRONMENT FOR APPLICATIONS TO RUN

Organizations face increasing pressure to acquire and operate integrated and efficient applications. It is crucial for modern companies to establish a secure environment for these applications, particularly for critical components such as operating systems, email, and messaging services.

These components can be sourced from service providers or developed internally. Furthermore, it is crucial for management to actively monitor the organization's infrastructure after implementation, instead of solely relying on the IT department for oversight.

PROTECTING DATA COLLECTED AND USED BY ORGANIZATIONS

Data is crucial for organizations as it underpins their ability to conduct transactions and provide value to consumers. In today's interconnected environment, effective information systems are essential for businesses, educational institutions, and government entities.

These information systems not only facilitate the development and transfer of goods and services but also require the protection of data both in motion and at rest to ensure comprehensive information security.

The value of data makes it a target for attackers who may seek to steal, sabotage, or corrupt it. Consequently, the integrity and value of organizational data can be safeguarded through a well-implemented information security program overseen by the management of the organization.

KEEPING ORGANIZATIONAL TECHNOLOGY ASSETS SAFE

When an organization's network expands to meet new needs, more powerful technology solutions should take place of outgrown security measures. Organizational development, for example, may need the implementation of public key infrastructure (PKI), used to create and manage public keys for encryption, which is a common method of securing data transfers on the internet.

A firewall, which keeps certain types of network traffic out of a private network, is an example of a robust solution.

Another example is caching network appliances, which are devices that store local copies of Internet material, such as frequently visited Websites. Rather than accessing the sites from the server each time, the appliance presents the cached pages to users.

THREATS

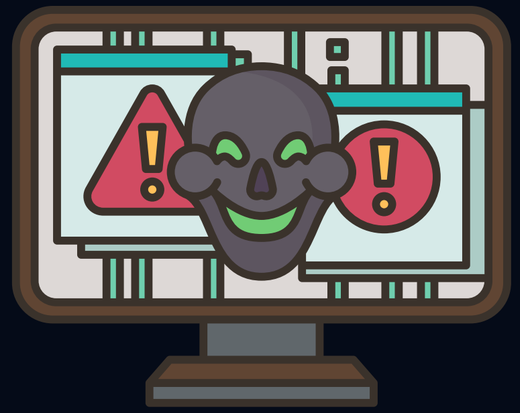
Management must be aware on the numerous dangers to an organization's people applications, data, and information systems in order to make informed decision about information security.

To safeguard your organization's data, you must understand yourself, that is be familiar with the data to be protected as well as the systems that store, transport, and process it; and second, to understand the dangers you face.

WHAT IS A THREAT?

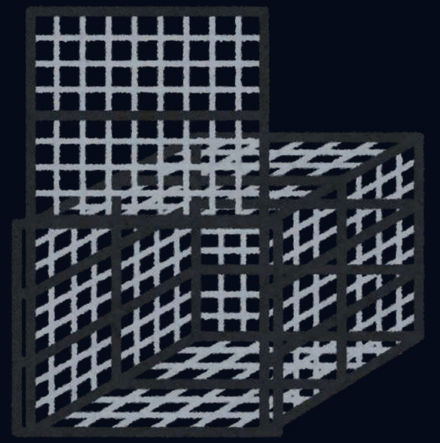
A threat is an object, person, or other thing that poses a continuing threat to an asset in the context of information security.

Comprises to Intellectual Property – piracy, copyright infringement,



Software attacks – viruses, worms, denial of service

Espionage or Trespass – Unauthorized access and/or illegal data collection

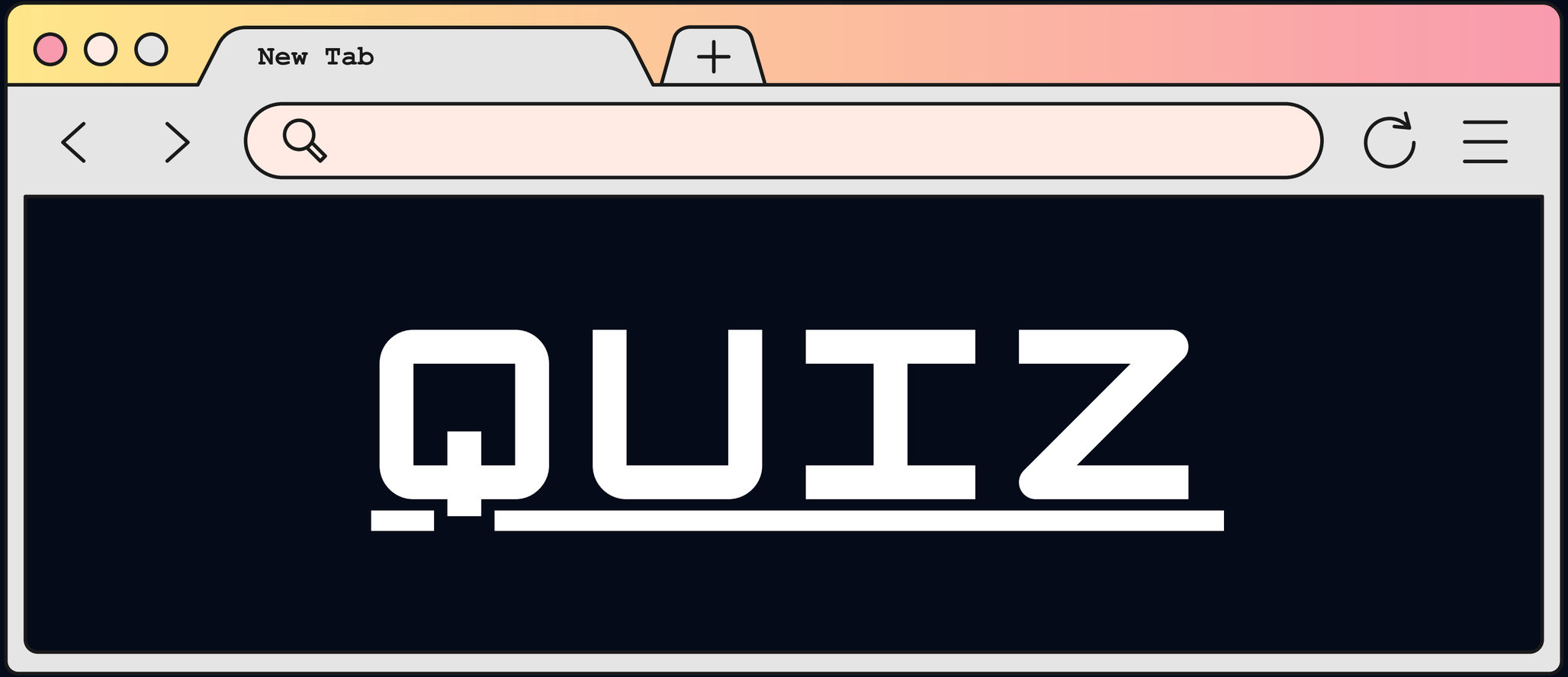


Sabotage or Vandalism – Destruction of systems or Information

Technological obsolescence – Outdated Technologies or equipment for information security

Information Extortion – Blackmail, Information disclosure

Missing, Inadequate, or Incomplete controls – Network compromised because no firewall security is present or no control over it


New Tab
QUIZ

New Tab

What is Information Security?

1. What is the primary goal of an information security program?

a. To update systems regularly
b. To ensure that systems and their contents remain the same
c. To acquire the latest technology
d. To reduce the cost of IT operations

New Tab

What is Information Security?

2. Which of the following is NOT a critical function of information security for a company?

a. Keeping the company's ability to function safe
b. Ensuring applications are safe to use
c. Reducing the number of employees
d. Keeping the company's technological assets safe

New Tab

What is Information Security?

3. Information security is primarily a concern of:

a. General management only
b. IT management only
c. Both general and IT management
d. External security consultants

New Tab

What is Information Security?

4. What should organizations focus on when managing information security?

a. Implementing the latest technological tools
b. Formulating and enforcing policies
c. Hiring more IT personnel
d. Outsourcing security to third parties

New Tab

What is Information Security?

5. Why is it important to establish a secure environment for applications in an organization?

a. To ensure the smooth operation of critical components like operating systems and messaging services
b. To reduce the costs associated with IT maintenance
c. To simplify the organization’s IT infrastructure
d. To limit the use of external service providers

New Tab

What is Information Security?

6. What makes organizational data a target for attackers?

a. Its lack of encryption
b. The ease of accessing it
c. Its value in conducting transactions and providing consumer value
d. The outdated systems it resides on

New Tab

What is Information Security?

7. Which technology solution is used to create and manage public keys for encryption?

a. Firewall
b. Caching network appliance
c. Public Key Infrastructure (PKI)
d. Antivirus software

New Tab

What is Information Security?

8. What is a threat in the context of information security?

a. A minor inconvenience to IT systems
b. An object, person, or thing that poses a continuing danger to an asset
c. An outdated piece of technology
d. A temporary issue with software

New Tab

What is Information Security?

9. Which of the following is an example of a software attack?

a. Piracy
b. Denial of service
c. Unauthorized access
d. Blackmail

New Tab

What is Information Security?

10. What can lead to a network being compromised in terms of security?

a. Missing, inadequate, or incomplete controls
b. Regular software updates
c. Strong firewall protection
d. Frequent employee training