



INFORMATION SYSTEMS SECURITY

INTRODUCTION

Lecture One



JIMMY M.R.

Lecture Objectives

- In this lecture, one will learn:
  - Introduction to Information Systems Security
  - What We Are Securing
  - Properties of Information Systems Security
  - Security Controls
  - How to Calculate Systems Availability

Introduction to Information Systems Security

- An **Information System** consists of the hardware, operating system, and application software that work together to collect, process, and store data for individuals and organizations.
- **Information Systems Security** is the collection of activities that protect the information systems and the data stored in them.
- **System Security:** is the protecting of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.
- In a general sense, security means protecting our assets from attackers invading our networks, natural disasters, adverse environmental conditions, power failures, theft or vandalism, or other undesirable states.

© Muwa JR 2024 - - - rickmuwa@gmail.com

Concepts of Information Systems Security

- To make systems more secure, there is need to first understand the concepts of:
  - Risks
  - Threats
  - Vulnerabilities.

© Muwa JR 2024 - - - rickmuwa@gmail.com

Risk

- **Risk** is the likelihood that something bad will happen to an asset. It is the level of exposure to some event that has an effect on an asset.
- In the context of IT security, an asset can be a computer, a database, or a piece of information.
- Examples of risk include the following:
  - Losing data
  - Losing business because a disaster has destroyed your building
  - Failing to comply with laws and regulations

© Muwa JR 2024 - - - rickmuwa@gmail.com

Threat

- A **threat** is any action that could damage an asset. Information systems face both **natural** and **human-induced** threats.
- Natural threats like floods, earthquakes, or severe storms require organizations to create plans to ensure that business operation continues and that the organization can recover.
- A **Business Continuity Plan** (BCP) gives priorities to the functions an organization needs to keep going.

Threat

- A **Disaster Recovery Plan** (DRP) defines how a business gets back on its feet after a major disaster such as a fire or hurricane.
- Human-caused threats to a computer system include **viruses**, **malicious code**, and **unauthorized access**.
- A virus is a computer program written to cause damage to a system, an application, or data.
- Malicious code, or malware, is a computer program written to cause a specific action to occur, such as erasing a hard drive.
- These threats can harm an individual, business, or organization.

© Muwa JR 2024 - - - rickmuwa@gmail.com

Vulnerability

- A **vulnerability** is a weakness that allows a threat to be realized or to have an effect on an asset.
- For example: lighting a fire in a grill is not necessarily bad if one is cooking a meal. On the other hand, lighting a fire in a computer data center will likely cause damage.
- Therefore, a threat by itself does not always cause damage; there must be a vulnerability for a threat to be realized.

Vulnerability

- Vulnerabilities can often result in legal liabilities. Any vulnerability that allows a threat to be realized may result in legal action.
- Since computers must run software to be useful, and since humans write software, software programs inevitably contain errors. Thus, software vendors must protect themselves from the liabilities of their own vulnerabilities with an **End-User License Agreement** (EULA).
- A EULA takes effect when the user opens the package and installs the software. All software vendors use EULAs.

What We Are Securing

- Privacy Data of Individuals
  - Name, address, date of birth
  - Social Security number
  - Bank name, account number
  - Credit card account number
  - Utility account number
  - Mortgage account number
  - Insurance policy number
  - Securities and brokerage account numbers

© Muwa JR 2024 - - - rickmuwa@gmail.com

What We Are Securing

- Corporate Intellectual Property
  - Trade secrets
  - Product development
  - Sales and marketing strategies
  - Financial records
  - Copyrights, patents, etc.

© Muwa JR 2024 - - - rickmuwa@gmail.com

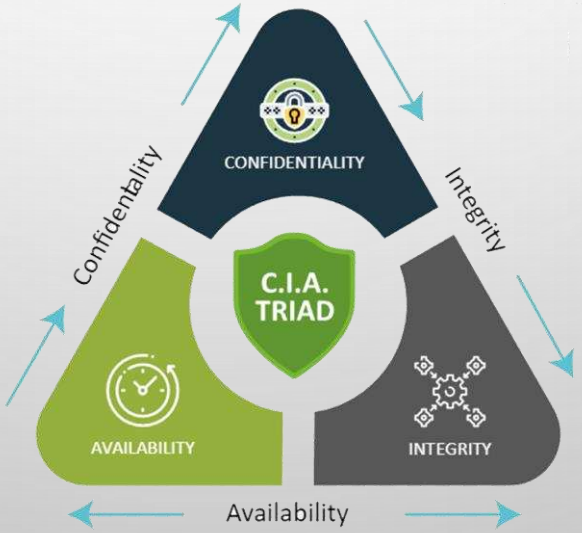
What We Are Securing

- Online B2C and B2B Transactions
  - Online banking
  - Online health care and insurance claims
  - E-commerce, e-government, services
  - Online education and transcripts
- Government Intellectual Property
  - National security
  - Military and DoD strategies

© Muwa JR 2024 - - - rickmuwa@gmail.com

Properties of Information Systems Security

- Information that is secure satisfies three main tenets, or properties, of information.
- **Confidentiality** - Only authorized users can view information.
- **Integrity** - Only authorized users can change information.
- **Availability** - Information is accessible by authorized users whenever they request the information.



Confidentiality

- **Confidentiality** means guarding information from everyone except those with rights to it. Confidential information includes the following:
  - Private data of individuals
  - Intellectual property of businesses
  - National security for countries and governments
- With the growth in E-commerce, more people are making online purchases with credit cards. This requires people to enter private data into E-commerce websites.
- Laws require organizations to use security controls to protect customers' private data. A **security control** is something an organization does to help reduce risk.

Confidentiality

- **Confidentiality** means guarding information from everyone except those with rights to it. Confidential information includes the following:
  - Private data of individuals
  - Intellectual property of businesses
  - National security for countries and governments
- With the growth in E-commerce, more people are making online purchases with credit cards. This requires people to enter private data into E-commerce websites.
- Laws require organizations to use security controls to protect customers' private data. A **security control** is something an organization does to help reduce risk.

Security Controls in Confidentiality

- Defining organization-wide policies, standards, procedures, and guidelines to protect confidential data. These are instructions for how to handle private data.
- Adopting a data classification standard that defines how to treat data throughout your IT infrastructure. This is the road map for identifying what controls are needed to keep data safe.
- Limiting access to systems and applications that house confidential data to only those authorized to use that data.

Security Controls in Confidentiality

- Using cryptography techniques to hide confidential data and keep that data invisible to unauthorized users.
- Encrypting data that cross the public Internet.
- Encrypting data that are stored within databases and storage devices.
- Conducting annual security awareness training for employees. This helps remind staff about proper handling of private data.
- Putting an IT security policy framework in place. A policy framework is like an outline that identifies where security controls should be used.

Security Controls in Confidentiality

- Designing a layered security solution for an IT infrastructure. The more layers or compartments that block or protect private data and intellectual property, the more difficult the data and property are to find and steal.
- Performing periodic security risk assessments, audits, and penetration tests on websites and IT infrastructure. This is how security professionals verify that they have properly installed the controls.
- Enabling security incident and event monitoring at your Internet entry and exit points. This is like using a microscope to see what is coming in and going out.

© Muwa JR 2024 - - - rickmuwa@gmail.com

Security Controls in Confidentiality

- Using more stringent access controls beyond a logon ID and password for sensitive systems, applications, and data. Access to more sensitive systems should have a second test to confirm the user's identity.
- Minimizing software weaknesses in your computers and servers by updating them with patches and security fixes.
- **Protecting private data is the process of ensuring data confidentiality**.

Security Controls in Confidentiality

- Sending data to other computers using a network means you have to take special steps to keep confidential data from unauthorized users.
- **Cryptography** is the practice of hiding data and keeping it away from unauthorized users.
- **Encryption** is the process of transforming data from cleartext into ciphertext.
- **Cleartext** data are data that anyone can read.
- **Ciphertext** is the scrambled data that are the result of encrypting cleartext.

Integrity

- **Integrity** deals with the validity and accuracy of data. Data lacking integrity—that is, data that are not accurate or not valid—are of no use.
- For some organizations, data and information are intellectual property assets. Examples include copyrights, patents, secret formulas, and customer databases. This information can have great value.
- Unauthorized changes can undermine the data's value.
- Sabotage and corruption of data integrity are serious threats to an organization, especially if the data are critical to business operations.

© Muwa JR 2024 - - - rickmuwa@gmail.com

Availability

- In the context of information security, **availability** is generally expressed as the amount of time users can use a system, application, and data.
- Common availability time measurements include the following:
- **Uptime** is the total amount of time that a system, application, and data are accessible. Uptime is typically measured in units of seconds, minutes, and hours within a given calendar month. Often uptime is expressed as a percentage of time available, e.g., 99.5 percent uptime.
- **Downtime** is the total amount of time that a system, application, and data are not accessible. Downtime also is measured in units of seconds, minutes, and hours for a calendar month.

Availability

- **Availability** is a mathematical calculation where A = (Total Uptime) / (Total Uptime + Total Downtime).
- **Mean time to failure** (MTTF) is the average amount of time between failures for a particular system. Semiconductors and electronics do not break and have an MTTF of many years (25 or more years, etc.). Physical parts such as connectors, cabling, fans, and power supplies have a much lower MTTF (five years or less), given that wear and tear can break them.
- **Mean time to repair** (MTTR) is the average amount of time it takes to repair a system, application, or component. The goal is to bring the system back up quickly.

© Muwa JR 2024 - - - rickmuwa@gmail.com

Availability

- **Mean time between failures** (MTBF) is the predicted amount of time between failures of an IT system during operation.
- **Recovery time objective** (RTO) is the amount of time it takes to recover and make a system, application, and data available for use after an outage. Business continuity plans typically define an RTO for mission-critical systems, applications, and data access.
- Telecommunications and Internet service providers offer their customers **service-level agreements** (SLAs). An **SLA** is a contract that guarantees a minimum monthly availability of service for wide area network (WAN) and Internet access links. Service providers typically offer SLAs ranging from 99.5 percent to 99.999 percent availability.

© Muwa JR 2024 - - - rickmuwa@gmail.com

How to Calculate Monthly Availability

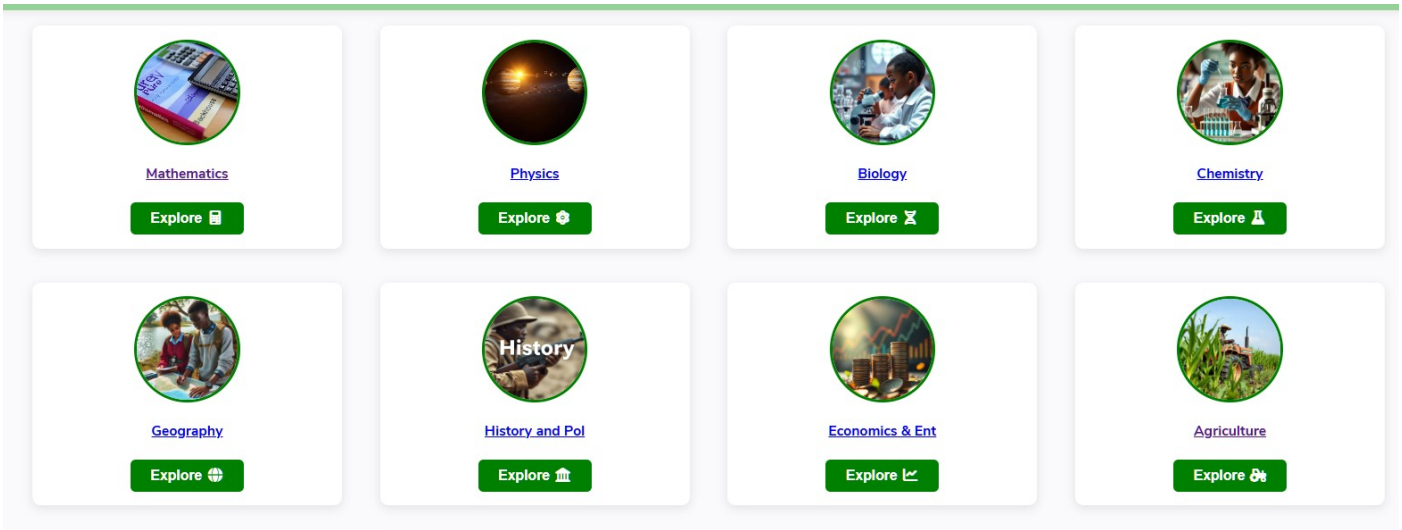
- For a given 30-day calendar month, the total amount of uptime equals:
- 30 days x 24 hours/day x 60 minutes/hour = 43,200 minutes
- For a 28-day calendar month (February), the total amount of uptime equals:
- 28 days x 24 hours/day x 60 minutes/hour = 40,320 minutes
- Using the formula Availability = (Total Uptime) / (Total Uptime + Total Downtime) calculate the availability factor for a 30-day calendar month with 30 minutes of scheduled downtime in that calendar month as:
- Availability = (43,200 minutes) / (43,200 minutes + 30 minutes) = 0.9993, or 99.93%

© Muwa JR 2024 - - - rickmuwa@gmail.com



© Muwa JR 2024 - - - rickmuwa@gmail.com

This document was downloaded from https://exoticnotes.com



NOTES for Secondary (S1 – S4)
https://exoticnotes.com/notes/secondary/o-level/

NOTES for Secondary (S5 – S6)
https://exoticnotes.com/notes/secondary/a-level/

PAPERS and Assessment items for Secondary (S1 – S6)
https://exoticnotes.com/papers/secondary/

Scenario Questions (with some Answers) (S1 – S6)
https://exoticnotes.com/scenario-questions

For New A level Curriculum (Notes, Assessment and Constructs, etc)
https://exoticnotes.com/new-a-level-curriculum

For New O level Curriculum (Notes, Scenarios, Papers, AOI, Syllabi, etc)
https://exoticnotes.com/new-o-level-curriculum