Introduction to Information Security

Module 1

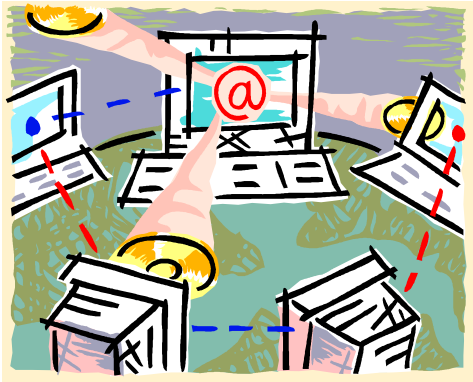
Objectives

- Definitions of information technology and information security
- Fundamental Security Concepts
- Ethics of IT Security

Definitions

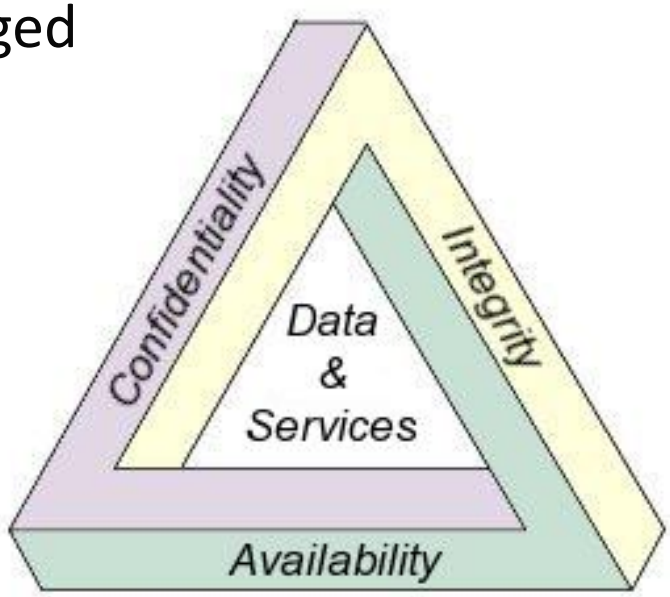
- Information Technology
  - Term used to describe computers and automated data processing

- Information Security
  - Protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability



CIA Triad

- Fundamental Characteristics
  - Confidentiality
    - Only those that should have access to data do
  - Integrity
    - Ensures the data has not be changed
  - Availability
    - Data is accessible when needed



http://en.wikipedia.org/wiki/CIA_triad

Confidentiality

- Assurance of data privacy
  - Only the intended and authorized recipients (individuals, processes, or devices) may access and read the data. Disclosure to unauthorized entities, for example using unauthorized network sniffing, is a confidentiality violation.
- Often provided through the use of cryptographic techniques

http://en.wikipedia.org/wiki/CIA_triad

Integrity

- Data integrity
  - Assurance that the information has not been altered or corrupted in transmission from source to destination, willfully or accidentally, before it is read by its intended recipient.
- Source integrity
  - Assurance the sender of the information is who it is supposed to be. Source integrity may be compromised when an agent spoofs its identity and supplies incorrect information to a recipient.
- Digital Signatures and hash algorithms are mechanisms used to provide data integrity

Availability

- Timely and reliable access to data services by authorized users
  - It ensures information or resources are available when needed; at a rate which is fast enough for the system to perform its intended task
- While confidentiality and integrity can be protected, an attacker may cause resources to become less available than required, or not available at all
- Robust protocols and operating systems, redundant network architectures, and system hardware without any single points of failure help to ensure system reliability and robustness
- A Denial of Service (DoS) attack is an attack against availability

Ethics of IT Security

Ten Commandments of Computer Ethics

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that insure consideration and respect for your fellow humans.

http://www.sans.org/reading_room/whitepapers/legal/legal-system-ethics-information-security_54

Ethics of IT Security

- Be a Good Online Citizen
  - **Safer for me, more secure for all:** What you do online has the potential to affect everyone – at home, at work and around the world. Practicing good online habits benefits the global digital community.
  - **Respect other online citizens:** Post only about others as you would have them post about you.
  - **Reference and Acknowledgment**: Represent authorship and reference others when using their ideas.
  - **Help the authorities fight cyber crime**: Report stolen finances or identities and other cybercrime to www.ic3.gov (Internet Crime Complaint Center), the Federal Trade Commission at http://www.onguardonline.gov/file-complaint.

http://www.staysafeonline.org/sites/default/files/resource_documents/STC%20tips%20and%20advice_0.pdf

Ethics of IT Security

- For more on online safety
  - http://www.staysafeonline.org/
  - http://www.cybercrime.gov/cyberethics.htm
  - http://www.onguardonline.gov/topics/net-cetera-heads-up-introduction.aspx
  - http://www.getnetwise.org/
  - http://xblock.isafe.org/
  - http://www.ikeepsafe.org/digital-citizenship/ethical-use/

True or False

1. Information security describes non-repudiation, availability, and confidentiality of computer systems.
2. An IT Security professional with authorized access is expected to snoop around their coworker's personal computer files.
3. Confidentiality, integrity, and availability are the fundamental concepts behind information security.
4. If data is not accessible, it is still secure as long as it has not been altered or deleted.
5. It is the responsibility of people who create and use the technology to make sure that it is utilized in a responsible and ethical manner.
6. Validation of sender is not necessary, as long as data is sent over a secure channel.

True or False

1. Information security describes non-repudiation, availability, and confidentiality of computer systems. TRUE
2. An IT Security professional with authorized access is expected to snoop around their coworker's personal computer files. FALSE
3. Confidentiality, integrity, and availability are the fundamental concepts behind information security. TRUE
4. If data is not accessible, it is still secure as long as it has not been altered or deleted. FALSE
5. It is the responsibility of people who create and use the technology to make sure that it is utilized in a responsible and ethical manner. TRUE
6. Validation of sender is not necessary, as long as data is sent over a secure channel. FALSE

Summary

- Provided background on fundamental security concepts creating a framework of how to protect information systems
- Defined information technology and information security
- Discussed IT Ethics

List of References

- http://en.wikipedia.org/wiki/CIA_triad
- http://www.sans.org/reading_room/whitepapers/policyissues/498.php
- http://www.sharepointsecurity.com/content-130.html
- http://media.wiley.com/product_data/excerpt/29/07645393/0764539329.pdf
- http://www.sans.org/reading_room/whitepapers/legal/legal-system-ethics-information-security_54
- http://www.staysafeonline.org/sites/default/files/resource_documents/STC%20tips%20and%20advice_0.pdf