EECS 3482

Introduction to Computer Security

Introduction to Information/Computer Security

Instructor: N. Vlajic, Fall 2020

Learning Objectives

Upon completion of this material, you should be able to:

- Describe the key security requirements of confidentiality, integrity and availability (CIA).
- Describe the CNSS security model (McCumber Cube).
- Identify today's most common threats and attacks against information.
- Distinguish between different main categories of malware.

Required Reading

Computer Security, Stallings: Chapter 1

Computer Security, Stallings: Chapter 6

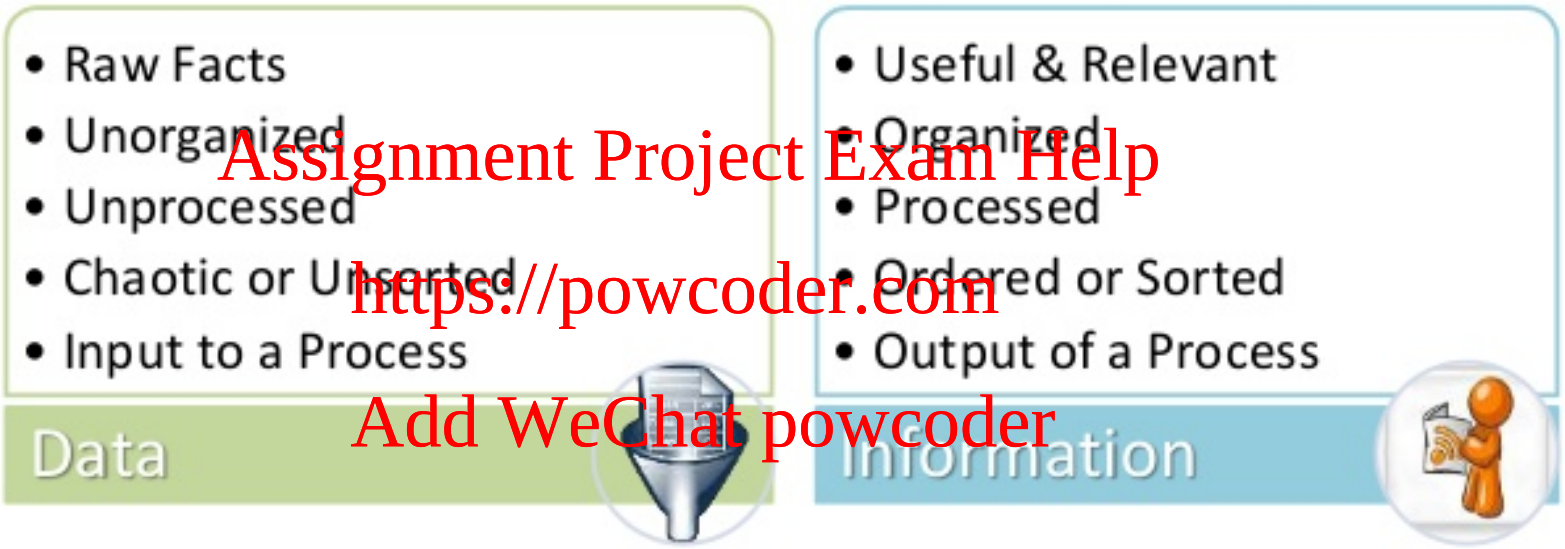
Introduction

- **Computer** – general purpose device that can be programmed to carry out a set of arithmetic or logical operations automatically
  - examples:
    - desktops
    - laptops, tablets
    - mobile phones
    - printers, servers
    - routers, firewalls
    - IoT devices
    - industrial controllers …

  - **alternative definition**: electronic device for storing and processing of data/information

Introduction (cont.)

- **Data vs. Information**

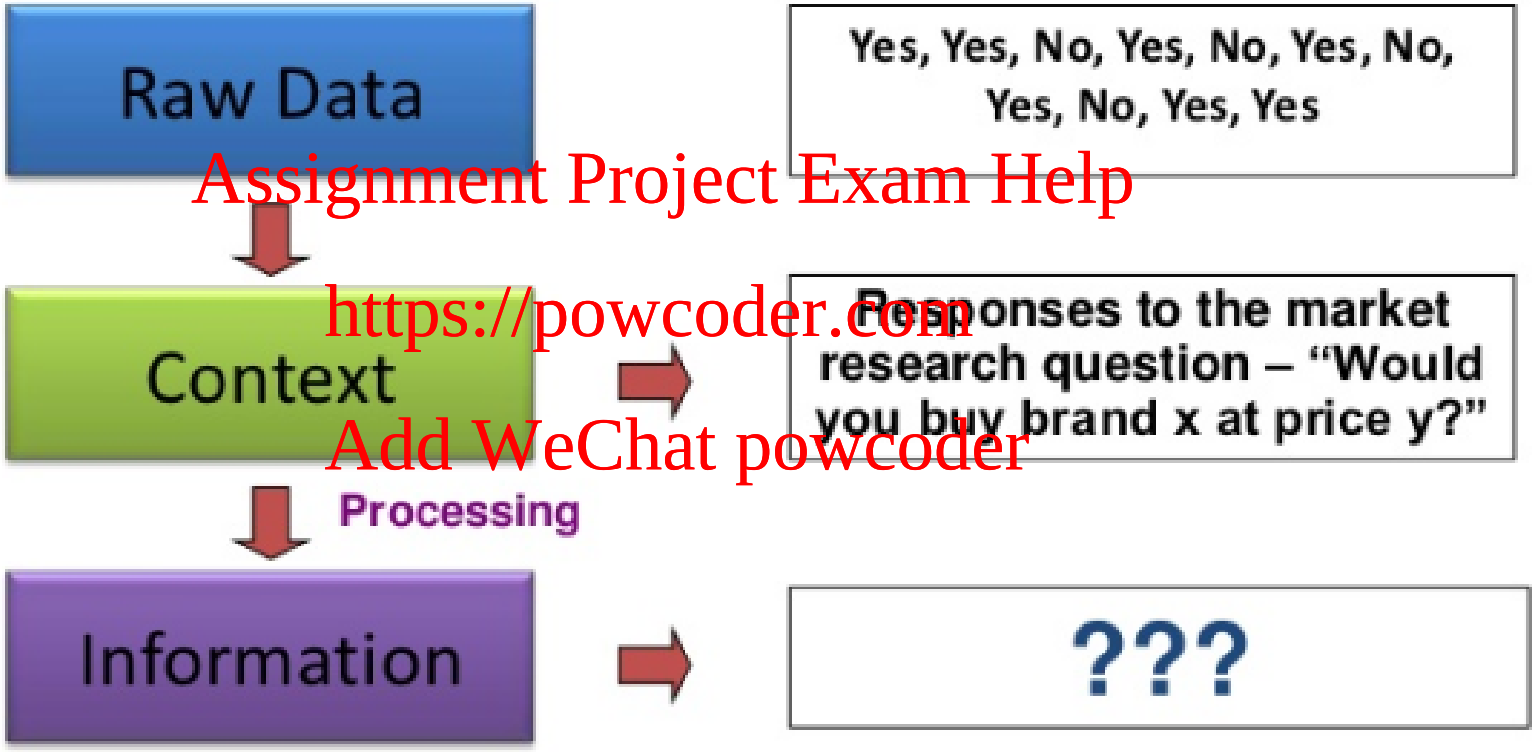


01000111 11101100 10100001
00111010 01011101 00001101
…

account balance: $238,000.00

In many organizations, information/data is seen as the most valuable asset !!!

Introduction (cont.)



http://www.slideshare.net/mrcox/btec-national-in-ict-unit-3-data-vs-information

Introduction (cont.)

Question:

Does compromise to/of data

always lead to

compromise of information??

Think of an encrypted file …

Introduction (cont.)

- **Information Technology** – technology involving development & use of computer systems & networks for the purpose of processing & distribution of data/information

  - categories of IT jobs:

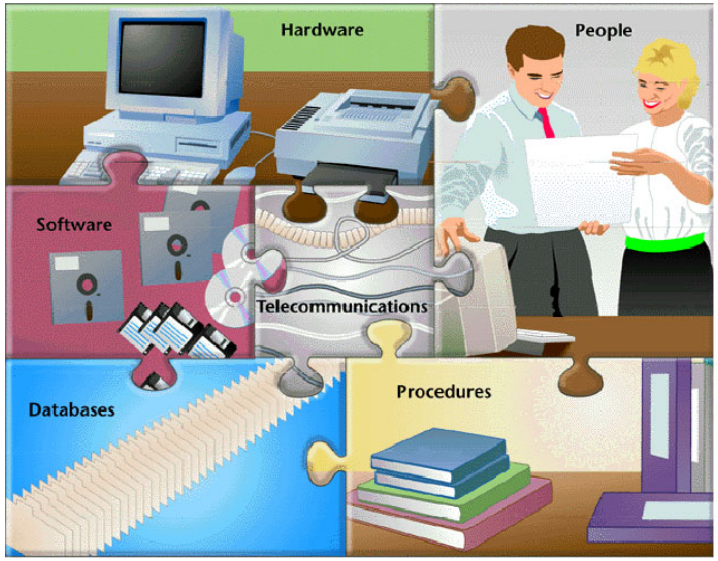
    - IT engineer - develops new or upgrades existing IT equipment (software or hardware)

    - IT architect - draws up plans for IT systems and how they will be implemented
    - IT administrator - installs, maintains, repairs IT equip./system
    - IT manager - oversees other IT employees, has authority to buy technology and plan budgets
    - IT security specialist - creates and executes security applications to maintain system security and safety

Introduction (cont.)

- **Information System** – entire set of data as well as software, hardware, networks, people, procedures & policies that deal with processing & distribution of information in an organization.

  - each component has its own strengths, weaknesses, and its own *security requirements*



Information/data is
- stored on computer hardware,
- manipulated by software,
- transmitted by networks,
- used by people,
- controlled by procedures & policies

Introduction (cont.)

Security = state of being secure, free from danger.

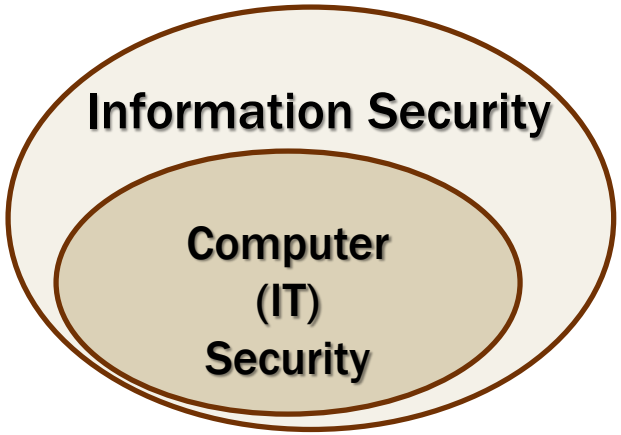
- **Information Security** – practice of defending digital information from unauthorized

  - access
  - use
  - recording
  - disruption
  - modification
  - destruction, ...

C.I.A.

Introduction (cont.)

- **Computer Security vs. Information Security**
  - terms are often used interchangeably, but …
  - computer security (aka IT security) is mostly concerned with information in '**digital form**'
  - information security is concerned with information in any form it may take: electronic, print, etc.



Introduction (cont.)

Data Center Security is much more than digital

1. Build on the right spot.

avoid locations prone to earth-quakes, floods, hurricanes, … near high-ways and airports

3. Pay attention to walls.

4. Avoid windows.

6. Keep a 100-foot buffer zone around the site.

in case of deliberate vandalism …

13. Plan for secure air handling.

prevent overheating or injection of biological and chemical substances from outside

18. Prohibit food in the computer rooms.

spillages or infestation can lead to equipment / data damage

https://www.cisco-eagle.com/blog/2008/01/30/data-center-security-is-much-more-than-digital/

http://www.csoonline.com/article/2112402/physical-security/physical-security-19-ways-to-build-physical-security-into-a-data-center.html?page=3

Introduction (cont.)

CISSP®

Certified Information Systems Security Professional

Environmental and life safety controls

- **Class A** – fires are common combustibles such as wood, paper, etc. This type of fire is the most common and should be extinguished with water or soda acid.
- **Class B** – fires are burning alcohol, oil, and other petroleum products such as gasoline. They are extinguished with gas or soda acid. You should never use water to extinguish a class B fire.
- **Class C** – fires are electrical fires which are fed by electricity and may occur in equipment or wiring. Electrical fires are Conductive fires, and the extinguishing agent must be non-Conductive, such as any type of gas.
- **Class D** – fires are burning metals and are extinguished with dry powder.
- **Class K** – fires are kitchen fires, such as burning oil or grease. Wet chemicals are used to extinguish class K fires.

Introduction (cont.)

Must know!

- **Types of Fires & Fire Extinguishers**

Type (Fire / Extinguisher)	CLASS A Combustible materials (e.g. paper & wood)	CLASS B Flammable liquids (e.g. paint & petrol)	CLASS C Flammable gases (e.g. butane and methane)	CLASS D Flammable metals (e.g. lithium & potassium)	Electrical Electrical equipment (e.g. computers & generators)	CLASS F Deep fat fryers (e.g. chip pans) cooking oil	Comments
Water	✓	✗	✗	✗	✗	✗	Do not use on liquid or electric fires
Foam	✓	✓	✗	✗	✗	✗	Not suited to domestic use
Dry Powder	✓	✓	✓	✓	✓	✗	Can be used safely up to 1000 volts
CO2	✗	✓	✗	✗	✓	✗	Safe on both high and low voltage
Wet Chemical	✓	✗	✗	✗	✗	✓	Use on extremely high temperatures

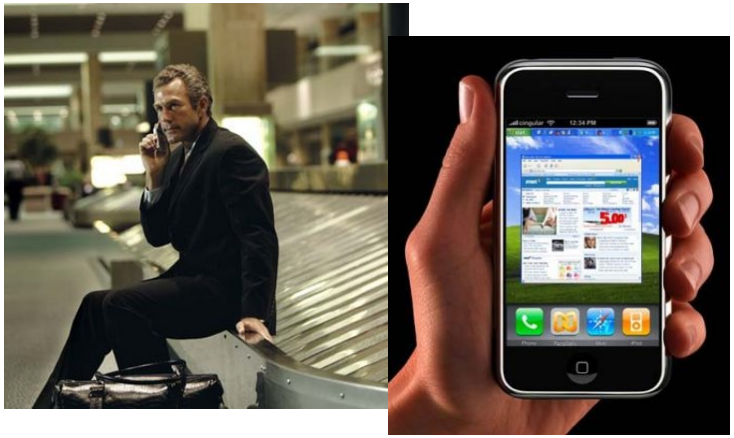
https://surreyfire.co.uk/types-of-fire-extinguisher/

Introduction (cont.)

Introduction (cont.)

- **Who is responsible for 'security of information'?**

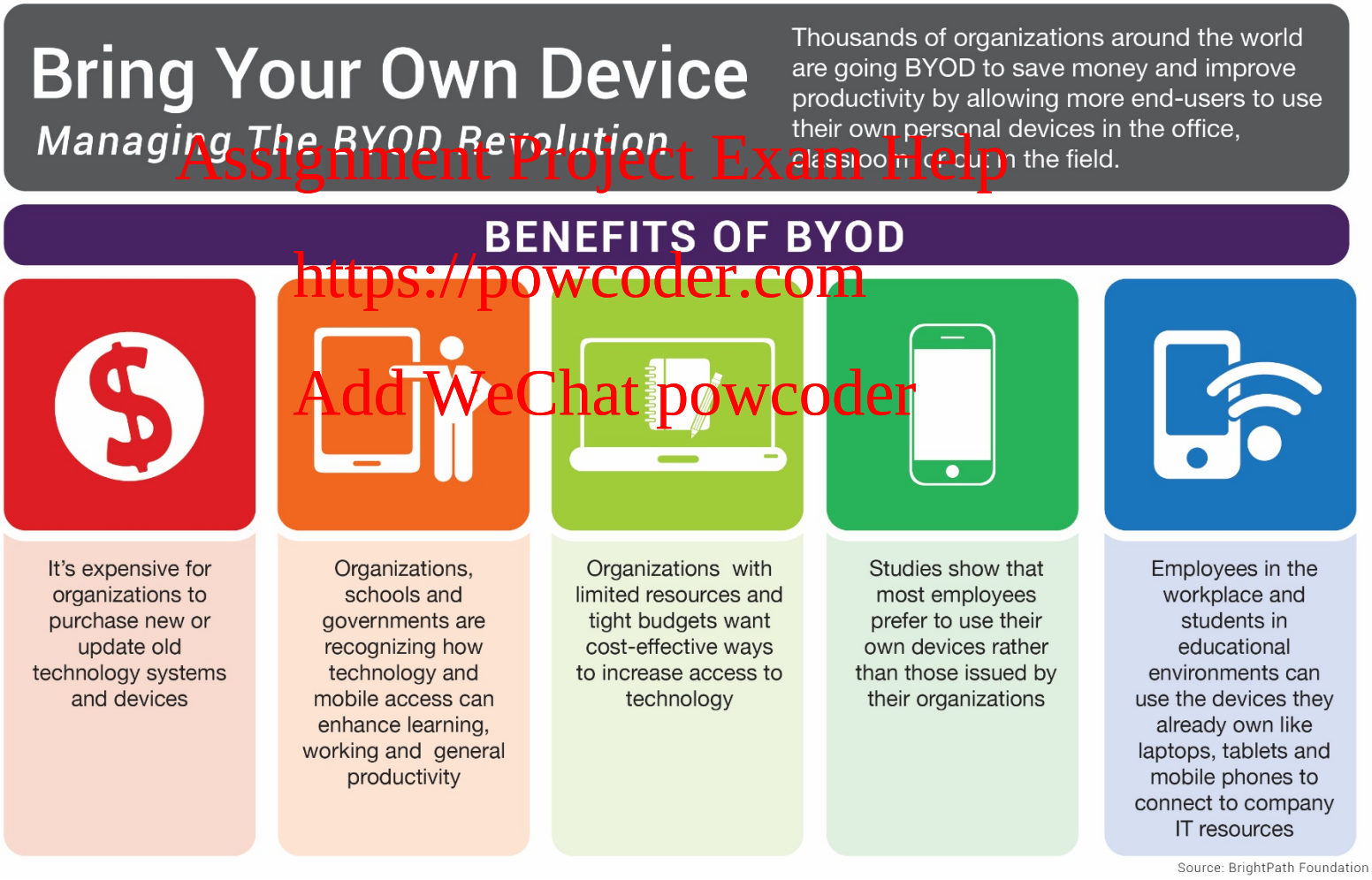
"In the last 20 years, technology has permeated every facet of the business environment. The business place is no longer static – it has changed as employees travel from office to office, from office to home, from city to city. Since business have become mobile, ... information security is no longer the sole responsibility of a small dedicated group of professionals, ..., it is now the responsibility of EVERY employee ...."



http://www.businessandleadership.com/fs/img/news/200811/378x/business-traveller.jpg
http://www.koolringtones.co.uk/wp-content/uploads/2010/01/mobile-phones.jpg

Introduction (cont.)

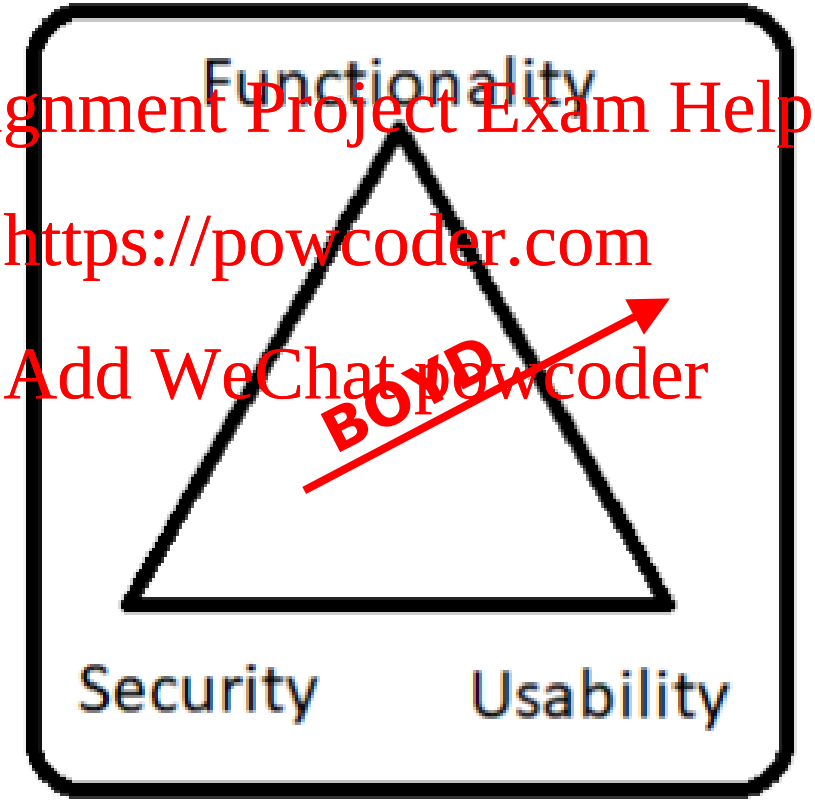
- **BYOD – the good and the bad**



http://lawinquebec.com/wp-content/uploads/2013/06/BYOD.jpg

Introduction (cont.)

- BYOD – the good and the bad (cont.)



3 main aspects of technology use.