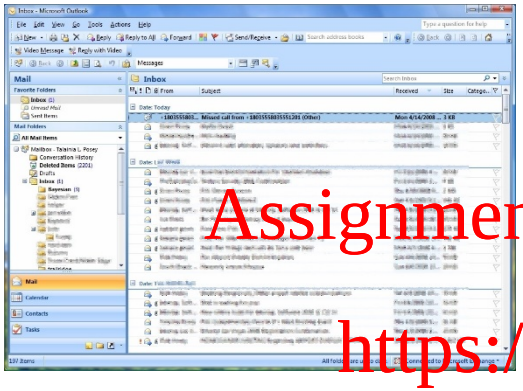


attack on integrity of software

can result in compromise of

- data confidentiality
- data integrity
- data availability

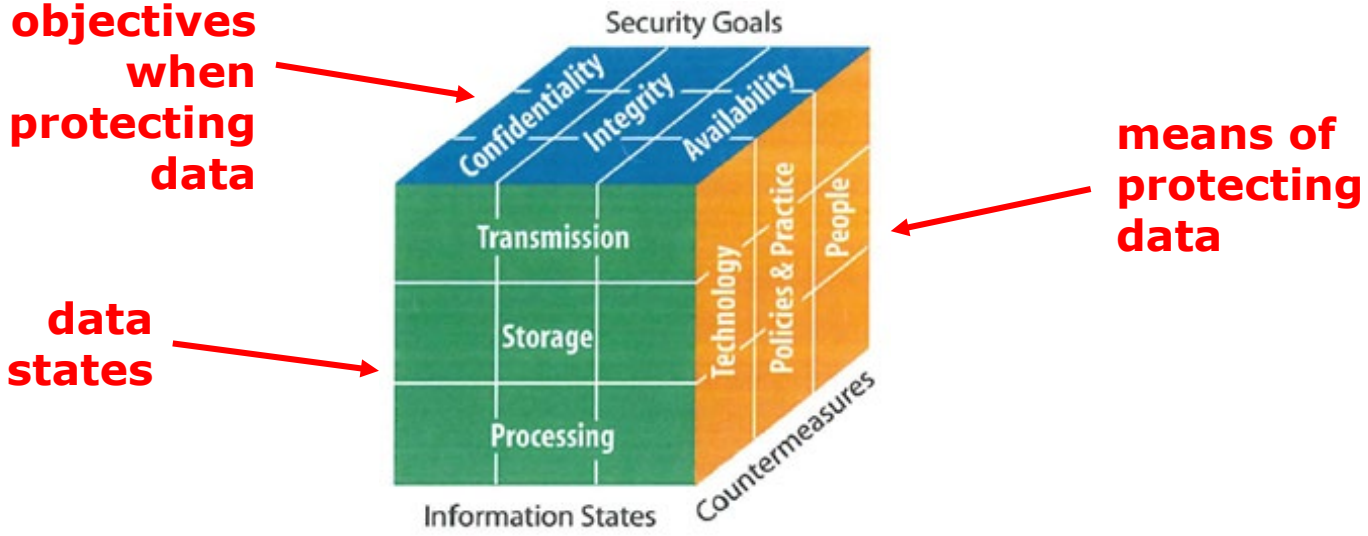
Where/how do we start building or evaluating a security system?

We know that we want to protect the CIA of data. But,

1) Data can reside in several different states.
2) Data can be attacked/protected in several different ways – e.g., through technology or through people.

CNSS Security Model

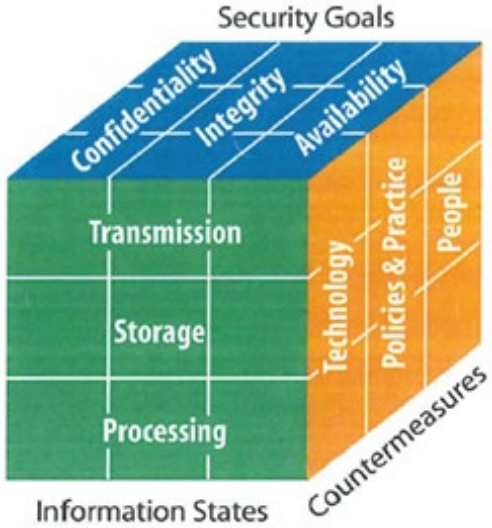
- **CNSS = Committee on National Security Systems**
- **McCumber Cube** – Rubik's cube-like detailed model for establishment & evaluation of info. security
  - to develop a secure system, one must consider not only key security goals (CIA) but also how these goals relate to various states in which information resides and full range of available security measures



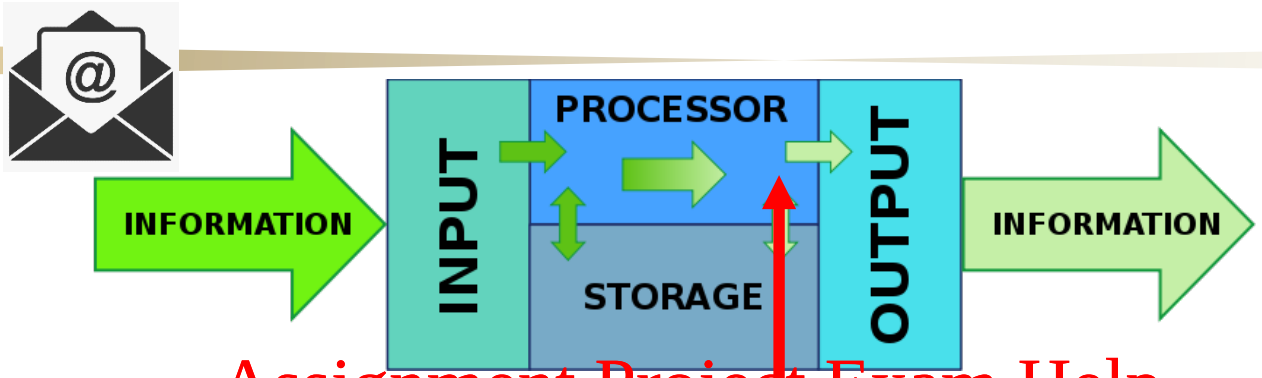
CNSS Security Model (cont.)

CNNS Category 2: Information States

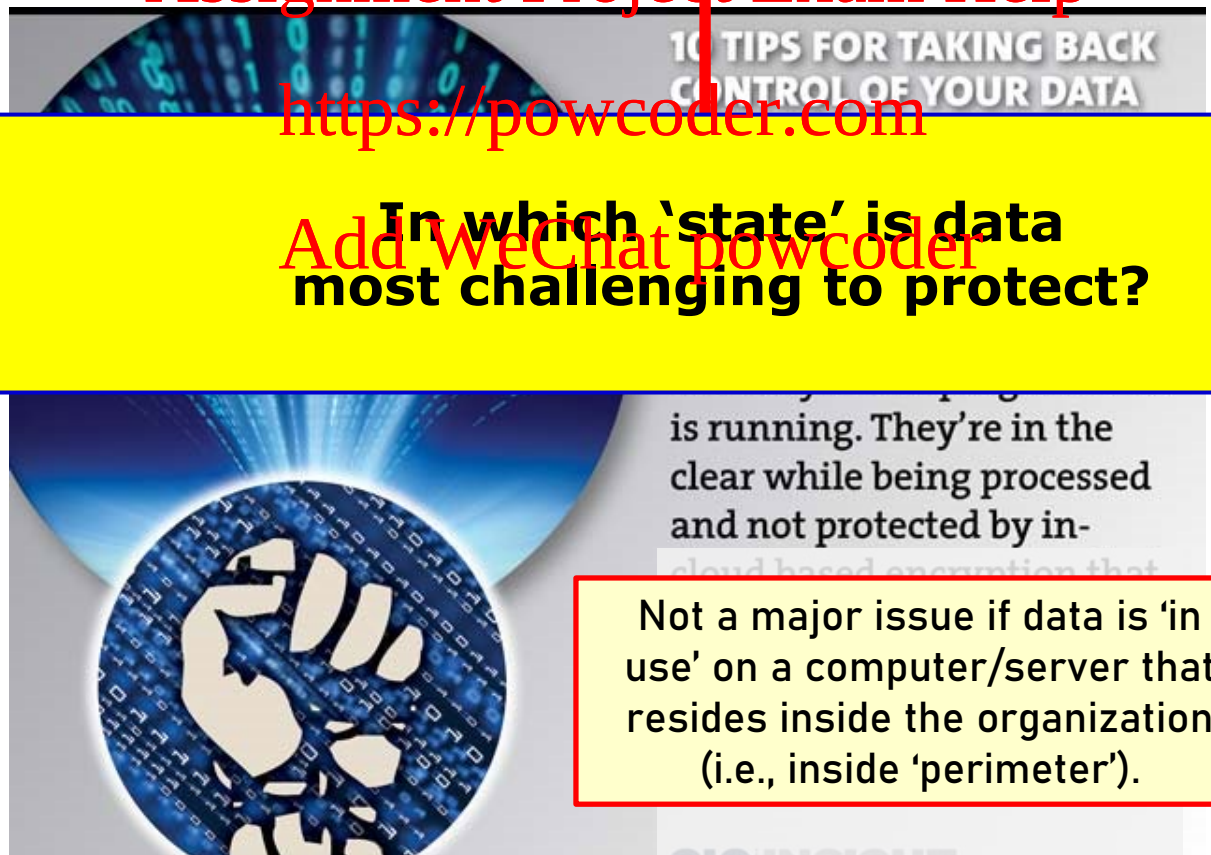
- **Storage** - aka '*data at rest*', such as data stored in memory or on a disk
- **Transmission** - aka '*data in transit*' - data being transferred between systems, in physical or electronic form
- **Processing** - aka '**data in use**' - data being actively examined or modified



CNSS Security Model (cont.)

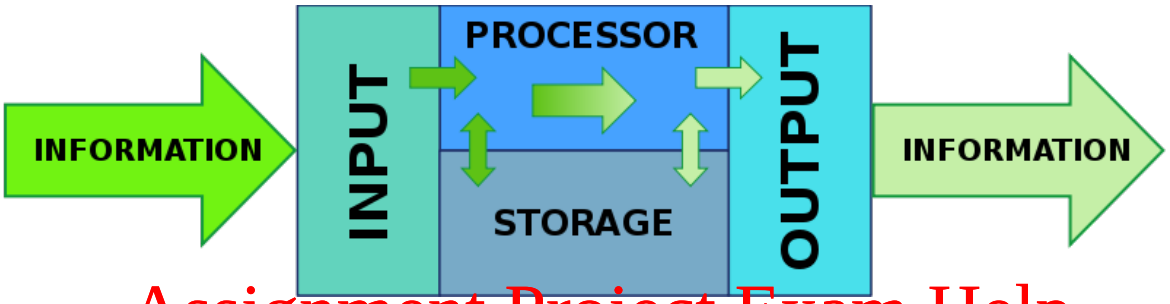


In which 'state' is data most challenging to protect?

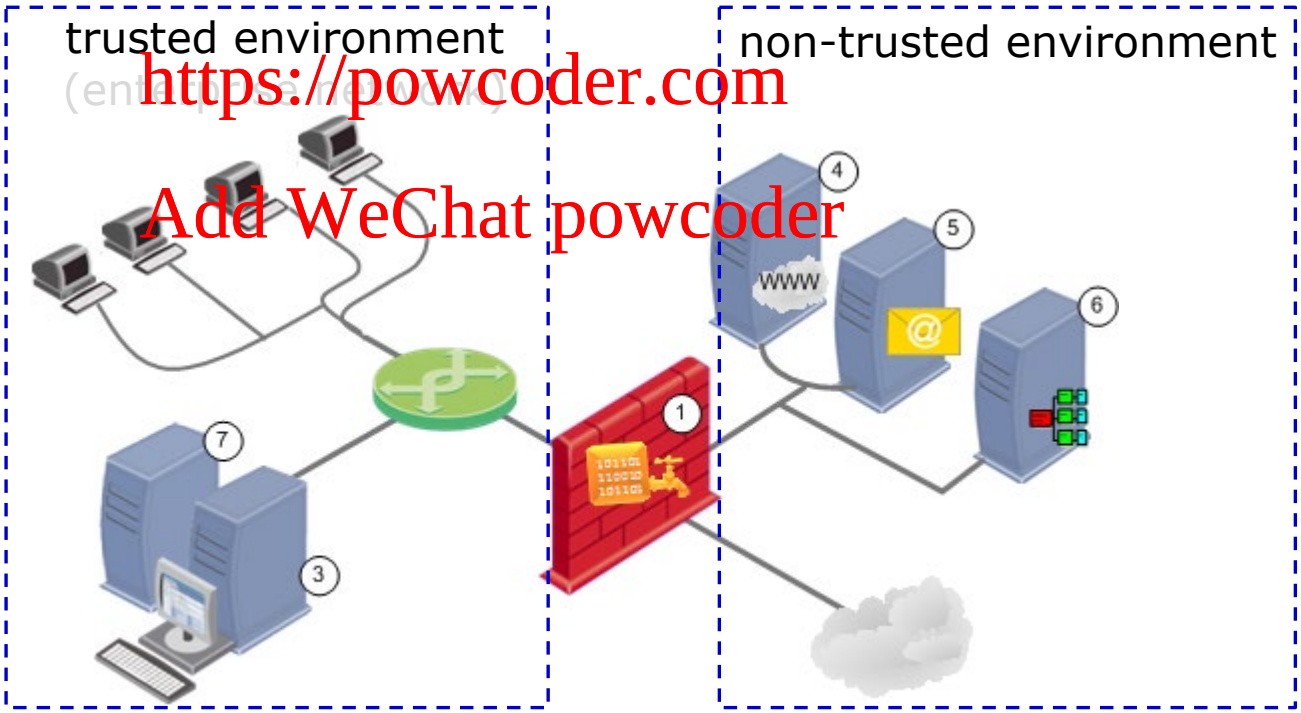


Not a major issue if data is 'in use' on a computer/server that resides inside the organization (i.e., inside 'perimeter').

CNSS Security Model (cont.)

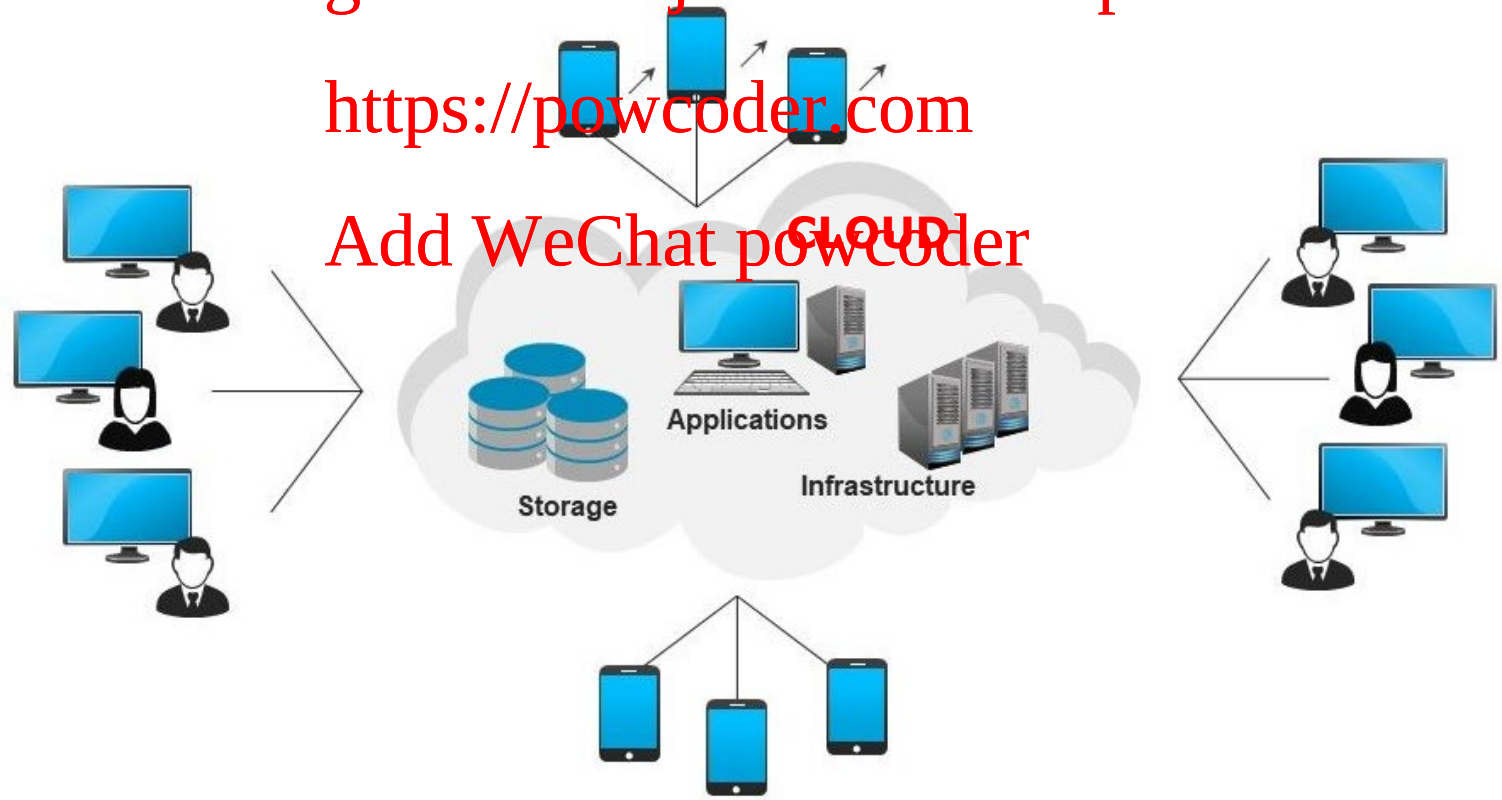


we can apply strong security controls (i.e., strong anti-virus protection) and minimize the chances of data being compromised while 'in use'



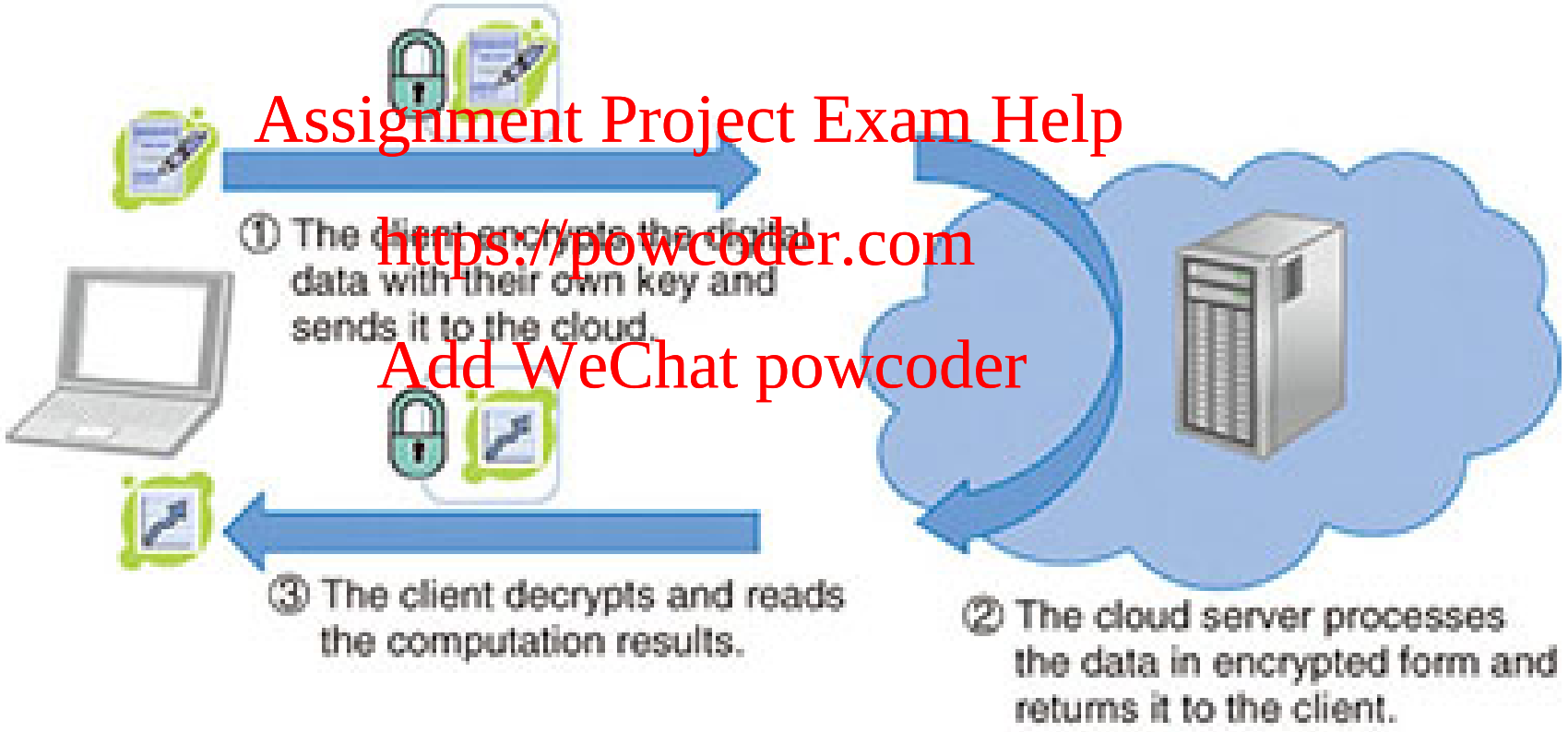
CNSS Security Model (cont.)

But, what if data is 'in use'
outside the trusted network/environment?!
(e.g., in case of Cloud Computing)



CNSS Security Model (cont.)

Example: Protection of Data in the Cloud

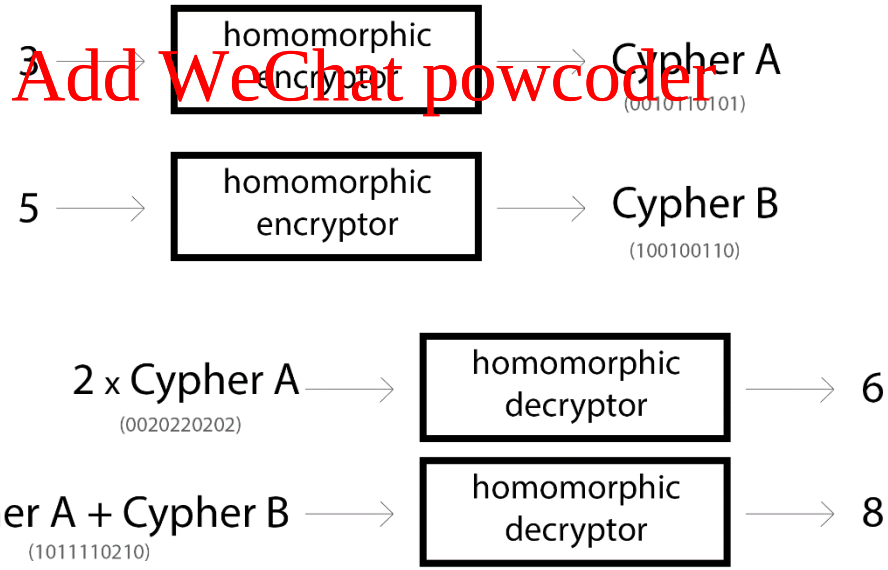


https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201407fa5.html

CNSS Security Model (cont.)

Example: Homomorphic Encryption

Homomorphic Encryption is a special type of encryption though. It allows someone to modify the encrypted information in specific ways *without being able to read the information*. For example, homomorphic encryption can be performed on numbers such that multiplication and addition can be performed on encrypted values without decrypting them. Here are a few toy examples.



https://iamtrask.github.io/2017/03/17/safe-ai/

CNSS Security Model (cont.)

Example: Homomorphic Encryption (cont.)

Performance

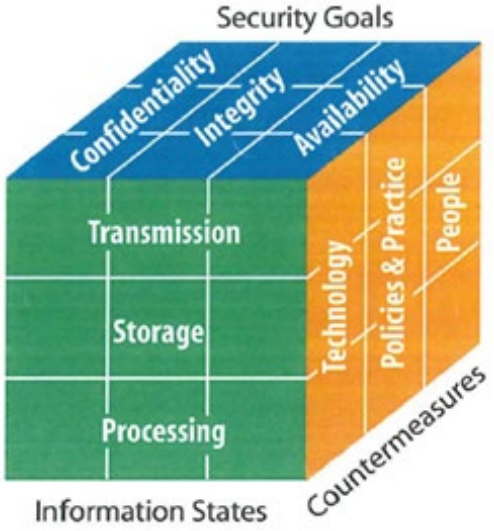
- A little slow…
- First working implementation in mid-2010, ½ -hour to compute a single AND gate
  - 13-14 orders of magnitude slowdown vs. computing on non-encrypted data
- A faster "dumbed down" version
  - Can only evaluate "very simple functions"
  - About ½-second for an AND gate

http://www.slideshare.net/NYTechCouncil/computing-on-encrypted-data

CNSS Security Model (cont.)

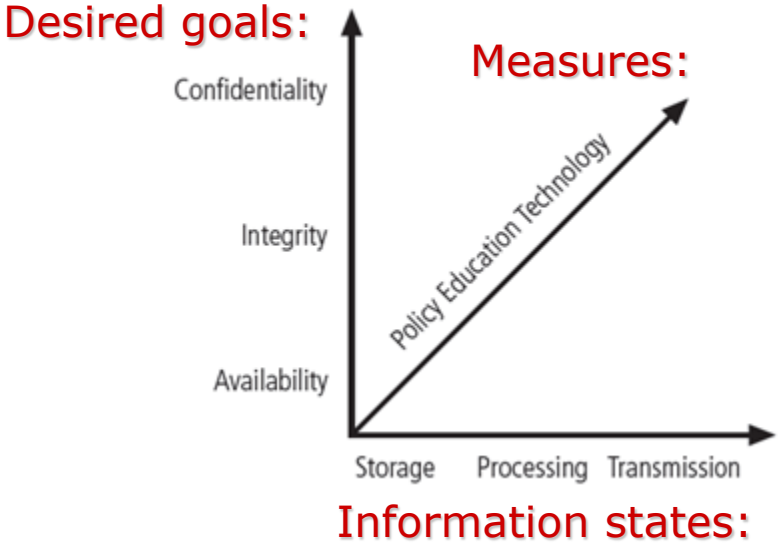
CNSS Category 3: Countermeasures/Safeguards

- **Technology** - software and hardware solutions (e.g., antivirus, firewall, IDS system, cryptography, backups, etc.)
- **People** - aka awareness, training, education - ensure that users are aware of their roles & responsibilities
- **Policy and practices** - administrative controls, such as management directives (e.g., acceptable use policies)



CNSS Security Model (cont.)

- Each of 27 cells in the cube represents an area that must be addressed to secure an information system
  - e.g., intersection between data integrity, storage and technology implies the need to use technology to protect data integrity of information while in storage
    - solution: new file check sum is calculated every time a critical file is modified …



CNSS Security Model (cont.)

Example: How to protect

- confidentiality of data
- while in transit (e.g., moved to/by USB)
- through education/awareness?

Scenario: An employee stores company information on a personal USB drive, in order to transfer it to another computer (e.g., work from home)

Safeguard: Educate employees about the importance of carefully handling data and encrypting data before transferring it to insecure 'movable' media – *in case that USB is infected or lost, encryption ensures that data cannot be read*

CNSS Security Model (cont.)

Are all 27 aspects of security worth investing into at every company?

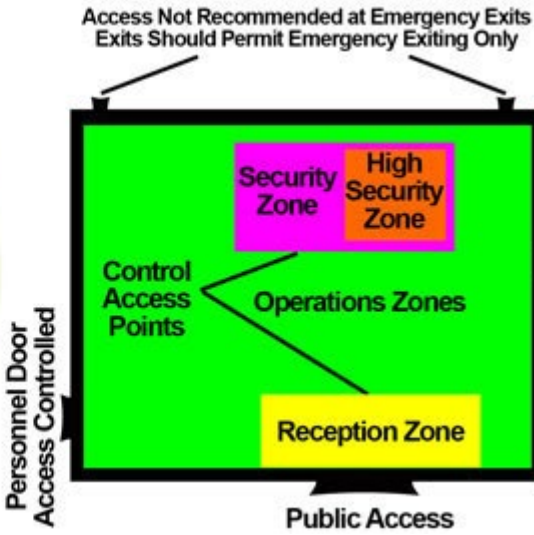
(could be too time consuming and/or too costly)

CNSS Security Model (cont.)

Example: Protecting Confidentiality of Data 'In Transit' Over Wireless Medium …

Busy downtown office:
Wifi used in an area that is within outside reach.

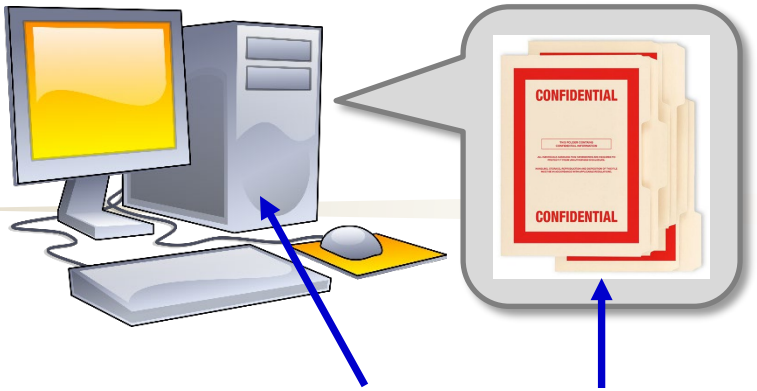
Remote nuclear plant:
WiFi used in an area that is NOT within outside reach.



Developing a 100% secure system would be great. But, most companies start developing their 'security systems/defences' by first understanding their most significant threats !!!

McCumber model is appropriate/excellent for evaluation but no so much for the design of a security system.

Threats



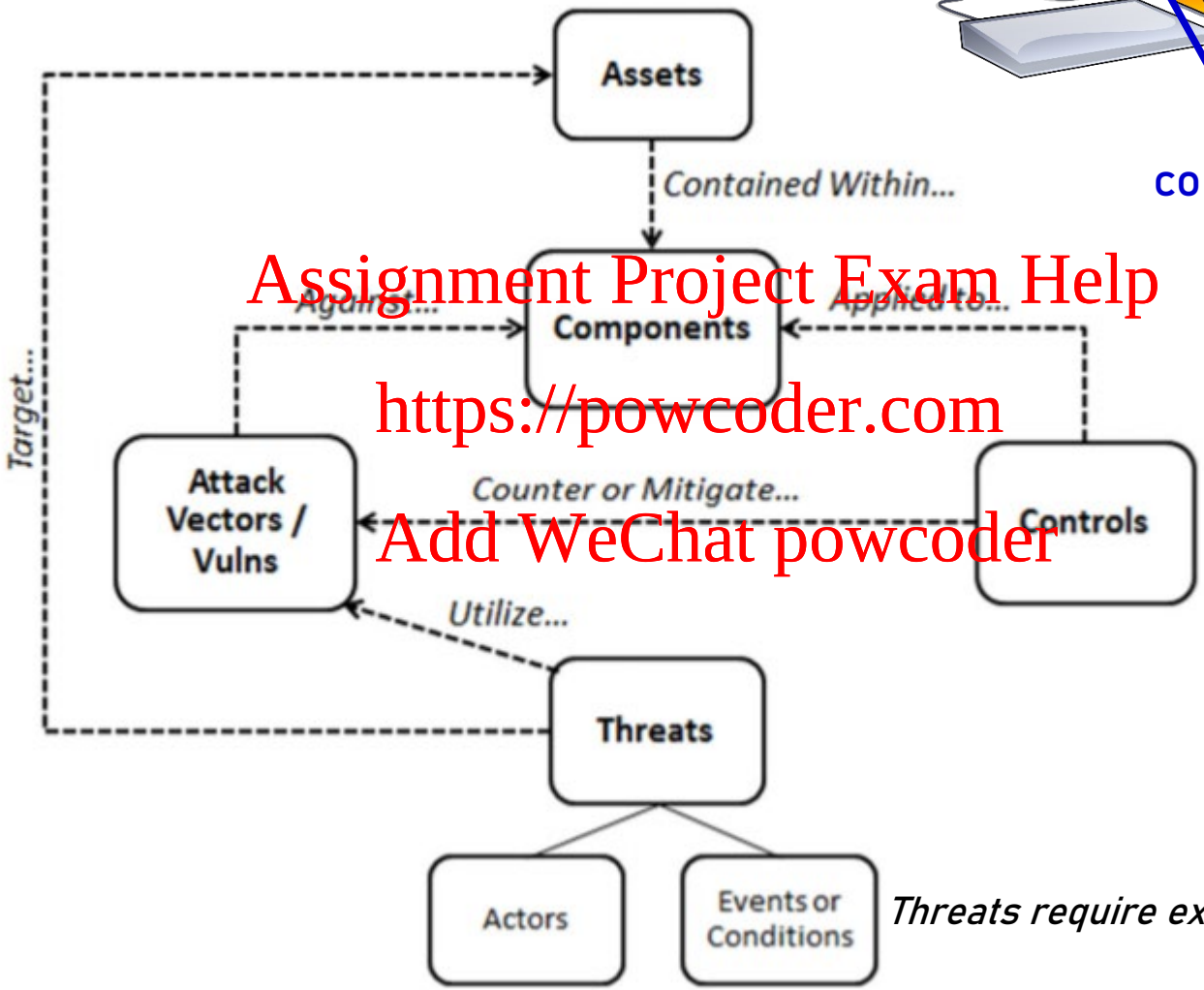


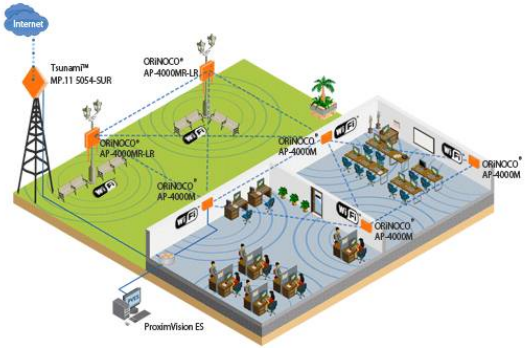
Figure 3 - Threats, Assets and Controls Relationship Model

https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Threat-Driven-Approach.pdf

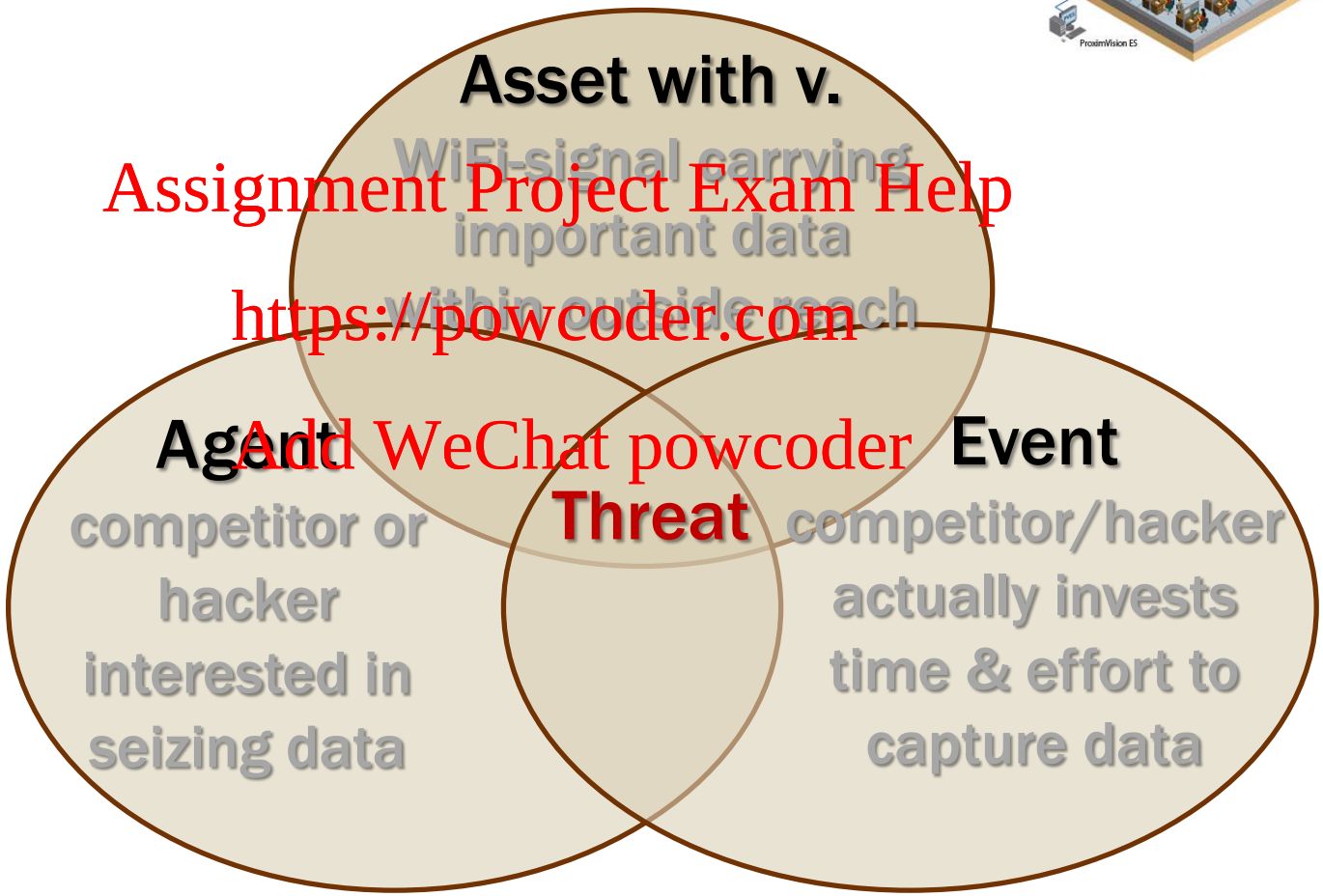
Threats (cont.)

- **Security Threat** - any event (action/inaction) that may or may not happen, but has the potential to cause disclosure, alteration, loss, damage or unavailability of a company's (or an individual's) assets
- Three main components of a security threat:
  - **Target** [asset / resource with vulnerability]: organization's system resource that might be attacked
    - information/data (its confidentiality, integrity, availability), software, hardware, communication facilities and networks, etc.
  - **Agent** [may or may not be present]: people/organizations originating the threat – intentional or non-intentional
    - employees, ex-employees, hackers, commercial rivals, terrorists, ...
  - **Event**: action that exploits target's vulnerability
    - malicious / accidental destruction or alteration of information, misuse of authorized information, etc.

Threats (cont.)



Example: Threat in WiFi network



NO EVENT ⇒ NO THREAT !!!