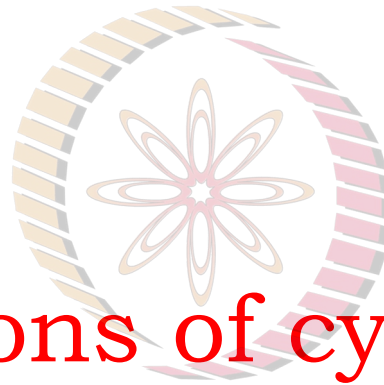


Cyber Security and Privacy

MS6880



Foundations of cyber security

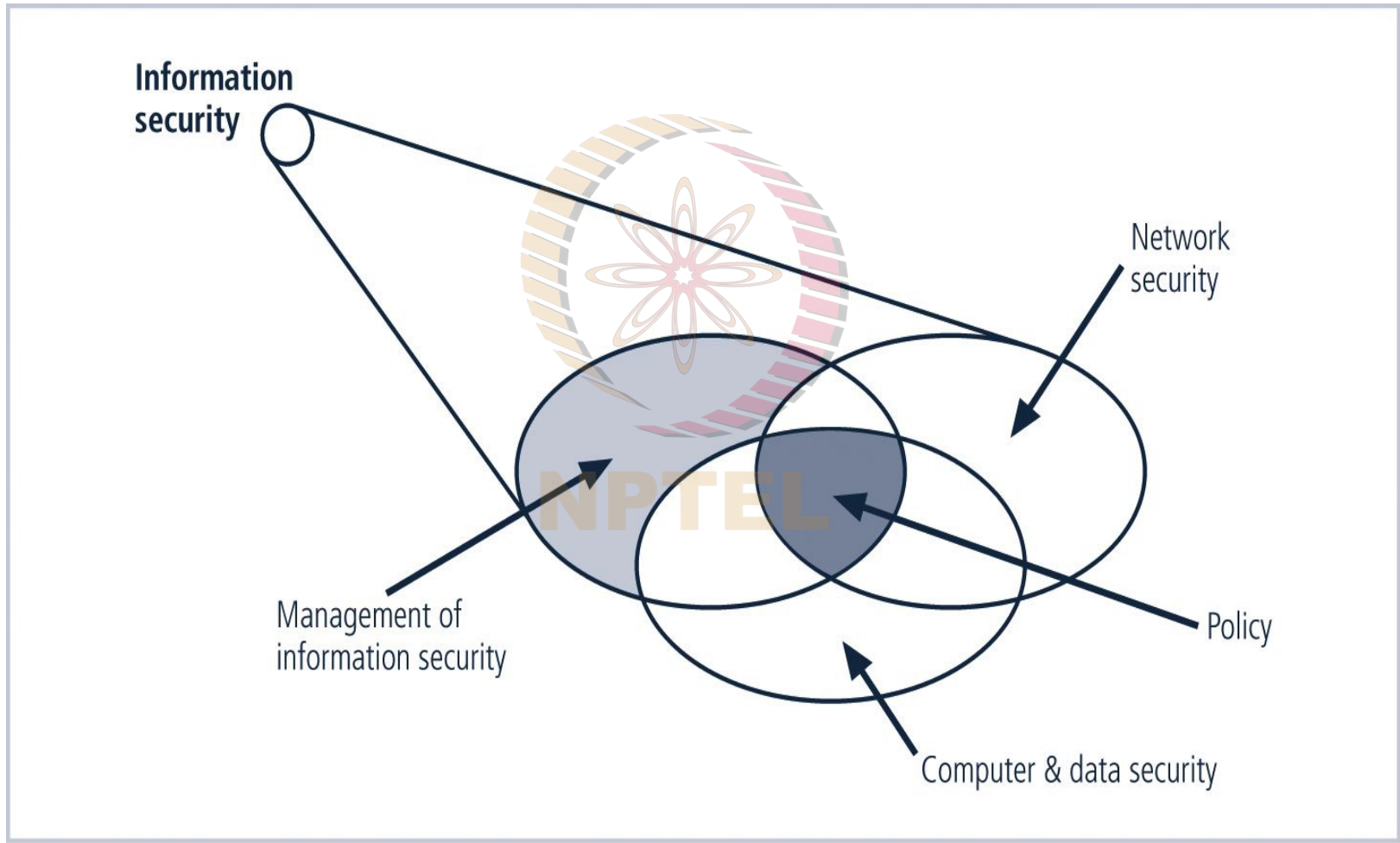
NPTEL

Saji K Mathew, PhD

Professor, Management Studies

INDIAN INSTITUTE OF TECHNOLOGY MADRAS

Components of Information Security



The CIA Triangle

- ▶ The C.I.A. triangle is made up of:

- ▶ **C**onfidentiality

- ▶ **I**ntegrity

- ▶ **A**vailability

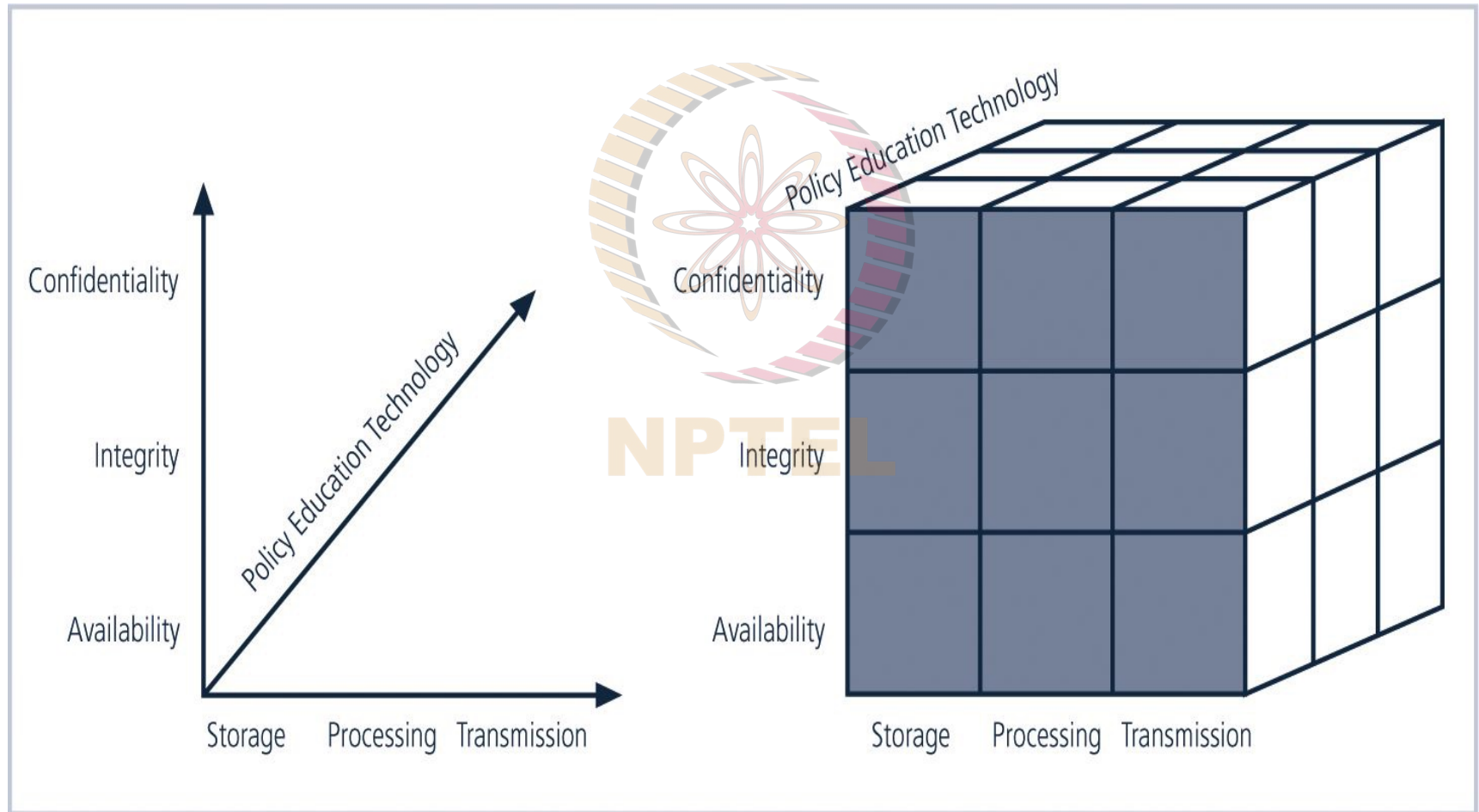


- ▶ Over time the list of characteristics has expanded, but these three remain central

- ▶ Identification, authentication and authorization are means to ensure CIA

NSTISSC Security Model

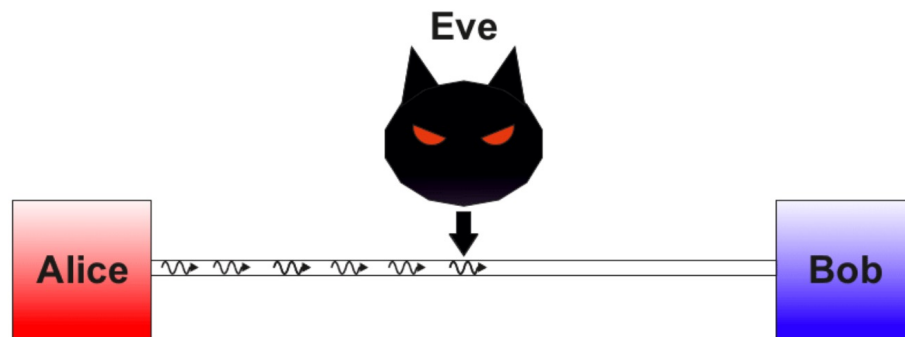
National Security Telecommunications and Info Sys Security Committee
(McCumber cube)



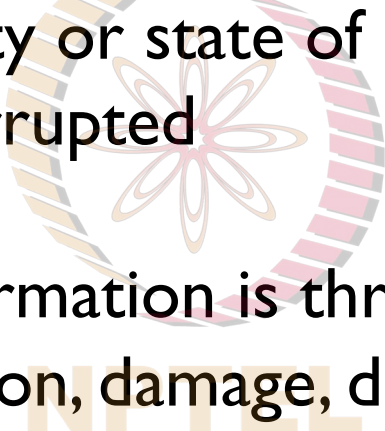
Confidentiality

- ▶ Confidentiality of information ensures that only those with sufficient privileges may access certain information
- ▶ In addition to cryptography, a number of measures may be used for confidentiality, including:
 - ▶ Information classification
 - ▶ Secure document storage
 - ▶ Application of general security policies
 - ▶ Education of information custodians and end users

(Rivest, Shamir and Adleman, 1978)



Integrity

- 
- The Intel logo is a circular emblem with a stylized flower-like shape in the center. The petals of the flower are in shades of pink and orange. The outer ring of the logo is composed of many small, overlapping segments in various colors, including yellow, orange, and pink. The word "INTEL" is written in a bold, sans-serif font across the middle of the logo.
- ▶ Integrity is the quality or state of being whole, complete, and uncorrupted
 - ▶ The integrity of information is threatened when it is exposed to corruption, damage, destruction, or other disruption of its authentic state
 - ▶ Corruption can occur while information is being compiled, stored, or transmitted
-

Availability

- ▶ Availability is making information accessible to user access without interference or obstruction in the required format
 - ▶ A user in this definition may be either a person or another computer system
 - ▶ Availability means availability to authorized users
-

Key Concepts of Information Security

► Identification

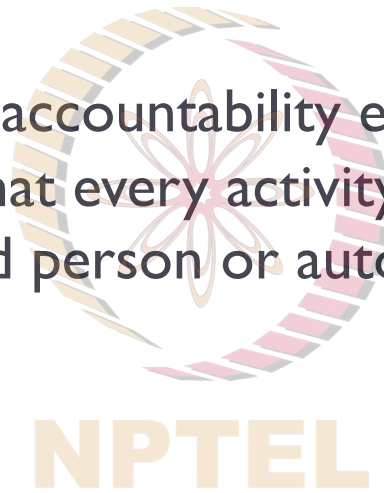
- Information systems possess the characteristic of identification when they are able to recognize individual users
- Identification and authentication are essential to establishing the level of access or authorization that an individual is granted



Key Concepts of Information Security

▶ Accountability

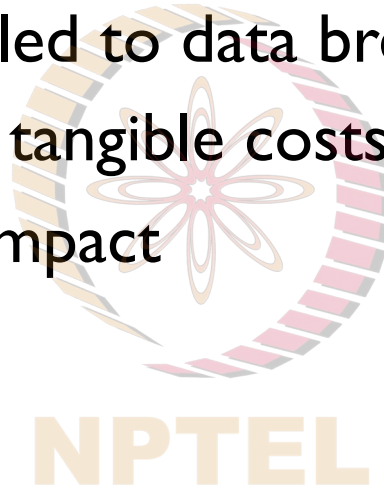
- ▶ The characteristic of accountability exists when a control provides assurance that every activity undertaken can be attributed to a named person or automated process





Target case questions (R4)

1. Identify: (i) Technological and (ii) Managerial vulnerabilities that led to data breach at Target
2. Enumerate Target's tangible costs vis-a-vis stakeholders
3. Identify intangible impact



NPTEL

BUSINESS LAW & ETHICS CORNER

Why you should care about the Target data breach



- ▶ Shortly before Thanksgiving 2013, someone installed malicious software (malware) on Target's security and payments system
- ▶ Designed to steal credit card data from the company's 1,797 U.S. stores
- ▶ In theory, Target was prepared for the hack: six months earlier, the company had begun installing a \$1.6 million malware detection tool designed to inform them of a data breach.

Target's security system

- ▶ **State of the art technology for security**
 - ▶ Used the same security system...employed by the CIA, the Pentagon, and other spy agencies around the world
 - ▶ Had multiple layers of protection-five firewalls, malware detection software, intrusion detection and prevention capabilities, and data loss prevention tools
 - ▶ **Performed internal and external validation and benchmarking assessments**
 - ▶ **Complied with data security standards in the credit card industry**
-

What went wrong?

- ▶ Hackers gained access to Target's system by stealing credentials provided by the company to Fazio Mechanical Services, a contractor that ran Target's climate systems.
 - ▶ Target failed to segment its network to ensure that Fazio—and other third parties—did not have access to its payment systems
 - ▶ Hackers exploited a connection designed to let Fazio exchange contract and project management information with Target
 - ▶ Used this connection to upload malware onto Target's systems, including its individual point-of-sale systems
-

The exploit

- ▶ The malware used by the hackers was programmed to steal Target's customer data at the point of sale
 - ▶ While payment information is encrypted when it is sent off to confirm a sale, it remains readable within the system
 - ▶ 'RAM scrappers' would copy customers' card information while it was still in the memory storage of Target's POS system
-

Impact

- ▶ What was the impact of the breach on Target?
 - ▶ Customers and banks have filed more than 90 lawsuits against Target
 - ▶ Customers, credit card companies, banks..
 - ▶ In numbers, Target's profit for the 2013 holiday shopping period fell 46% from the same quarter the year before
 - ▶ In sentiment, Target lost the trust of its customers, investors, and lenders.
-

Like the Titanic

- ▶ Target was warned repeatedly about the occurring cyberattack.
- ▶ Target's sophisticated security system could and should have addressed the malware uploaded by the hackers, but it failed to do so
- ▶ The system even had a function that would automatically delete malware as soon as it was detected, but Target's security team had turned off that function
 - ▶ Because it often halted email and Internet traffic by incorrectly flagging data as malware



Captain Smith's decisions

- ▶ Smith was not ignoring the ice warnings; he was simply not reacting to them. Ice warnings were just warnings that a ship sent saying that they had seen ice at a certain location (Kasprzak, 2012).
- ▶ Smith made the decision to not slow down the ship even though there were reports of ice (Barratt, 2010; Wilkinson & Hamilton, 2011).
 - ▶ The weather was calm and clear which gave no reason for Smith to slow the ship down
- ▶ Captain Smith also decided to leave the bridge to attend a dinner party



Only the paranoid survive

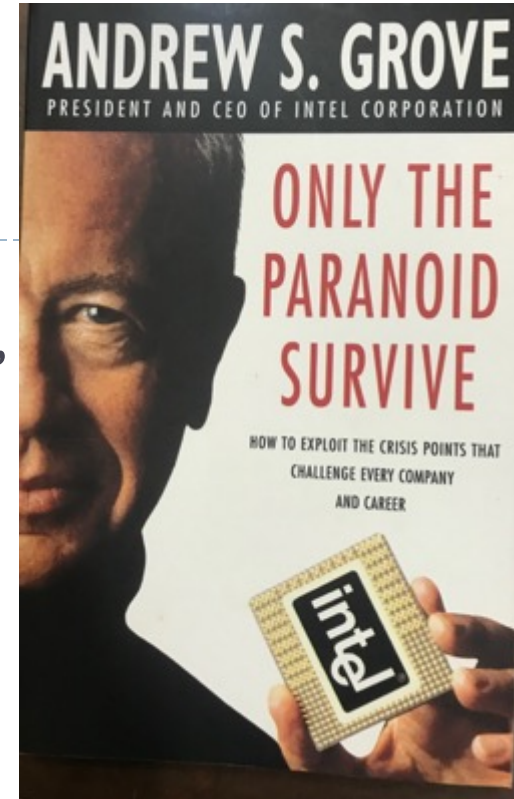
Added words to business vocabulary:

- ▶ “Inflection point”, “valley of death”, “10X force”

“I believe that the prime responsibility of a Manager is to guard constantly against other people’s attacks and to inculcate this guardian attitude in the people under his or her management”

“...I worry about factories not performing well, I worry about having too many factories. I worry about hiring the right people, and I worry about morale slacking off...”

--Andrew Grove, Former CEO, Intel Corporation



After effects

- ▶ Lesson on employee's ability to circumvent security
 - ▶ Move towards security management
 - ▶ Watershed moment in cyber security regulation
 - ▶ 52 laws related to data breach in the US, but no comprehensive national regulation; not one yet!
 - ▶ 0.1/72 for Target

“As long as the fines aren't putting businesses into bankruptcy—or even serious financial peril, for that matter—executives and boards are free to decide they are better off investing the bare minimum in security and saving the rest for possible breach costs and fines.” (An industry observer)
 - ▶ Is cyber security a god-talk* or a real concern?
-