A BRAND NEW WORLD!

Our Virtual Reality goes into High Gear

Welcome to our July 2020 Seminar

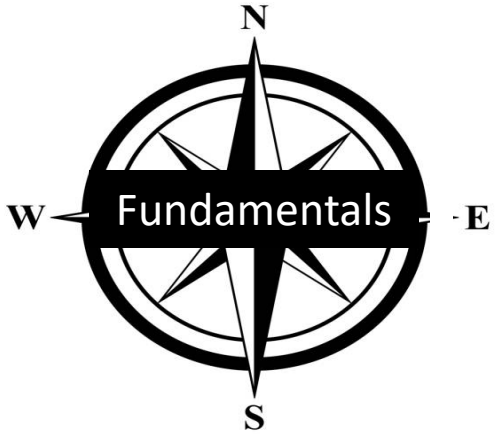
PROF. DR. JUAN CARLOS BARRERA

CYBER-SECURITY (BC6)

July 2020

Online Germany

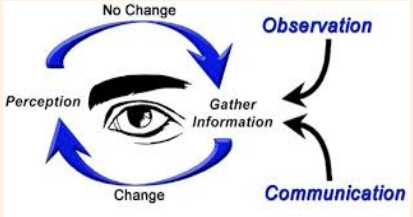
Broadcasting from USA

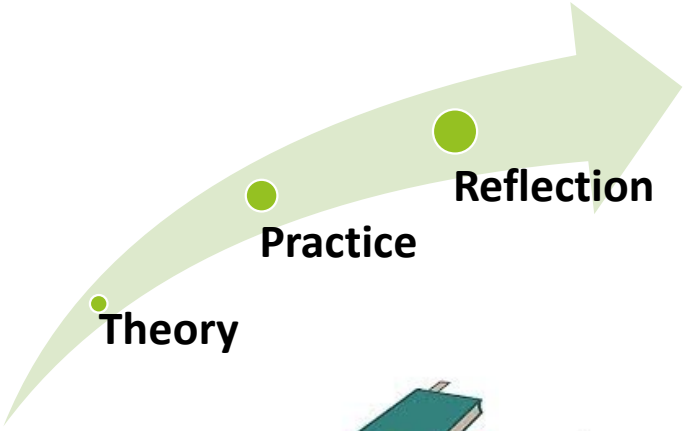


Fundamentals of Cybersecurity

Seminar Platform: www.learninglatitude.space

Virtual room: *Case Debriefings, Individual & Team exercises*

Coursework	**FUNDAMENTALS (1)**	**AWARENESS (2)**	**PREPARATION (3)**
Videos			
Teamwork	**RECOVERY (4)**	**DISCOVERY (5)**	**PROFICIENCY (6)**
Other			



Agenda:

1) The Importance of Context

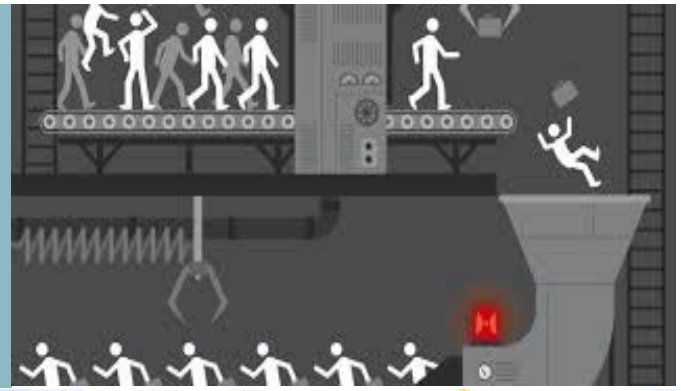
2) Videos: Discussion & Reflection

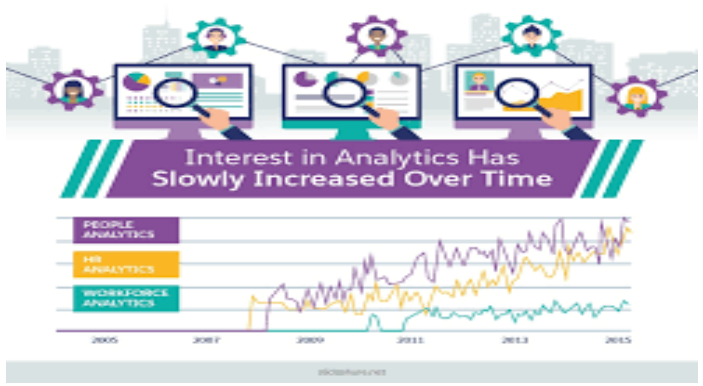
3) First Lab

4) The Need for Security

5) In Closing: Debriefings for Cases

1) The Importance of Context





Introduction

- Information security: a “well-informed sense of assurance that the information risks and controls are in balance.” —Jim Anderson, Inovant (2002)
- Necessary to review the origins of this field and its impact on our understanding of information security today

The History of Information Security

- Began immediately after the first mainframes were developed
- Created to aid code-breaking computations during World War II
- Physical controls to limit access to sensitive military locations to authorized personnel: badges, keys, and facial recognition
- Rudimentary in defending against physical theft, espionage, and sabotage

The History of Information Security

- One of 1st documented problems
  - Early 1960s
  - Not physical
  - Accidental file switch
    - Entire password file
    - printed on every output file

The 1960s

- Additional mainframes online
- Advanced Research Procurement Agency (ARPA) began to examine feasibility of redundant networked communications
- Larry Roberts developed ARPANET from its inception
- ARPANET is the first Internet

ARPANET Program Plan

June 3, 1968

In ARPA, the Program Plan is the master document describing a major program. This plan, which I wrote in 1968, had the following concepts:

1. **Objectives – Develop Networking and Resource Sharing**
2. **Technical Need – Linking Computers**
3. **Military Need – Resource Sharing - Not Nuclear War**
4. **Prior Work – MIT-SDC experiment**
5. **Effect on ARPA – Link 17 Computer Research Centers, Network Research**
6. **Plan - Develop IMP's and start 12/69**
7. **Cost – $3.4 M for 68-71**

ADVANCED RESEARCH PROJECTS AGENCY
Washington, D.C. 20301

Program Plan No. 723

Date: 3 June 1968

RESOURCE SHARING COMPUTER NETWORKS

A. Objective of the Program.

The objective of this program is twofold: (1) To develop techniques and obtain experience on interconnecting computers in such a way that a very broad class of interactions are possible, and (2) To improve and increase computer research productivity through resource sharing. By establishing a network tying IPT's research centers together, both goals are achieved. In fact, the most efficient way to develop the techniques needed for an effective network is by involving the research talent at these centers in prototype activity.

Just as time-shared computer systems have permitted groups of hundreds of individual users to share hardware and software resources with one another, networks connecting dozens of such systems will permit resource sharing between thousands of users. Each system, by virtue of being time-shared, can offer any of its services to another computer system on demand. The most important criterion for the type of network interconnection desired is that any user or program on any of the networked computers can utilize any program or subsystem available on any other computer without having to modify the remote program.

Courtesy of Dr. Lawrence Roberts

ARPANET Program Plan[4]

The 1970s and 80s

- ARPANET grew in popularity as did its potential for misuse
- Fundamental problems with ARPANET security were identified
  - No safety procedures for dial-up connections to ARPANET
  - Non-existent user identification and authorization to system

R-609

- Information security began with Rand Report R-609 (paper that started the study of computer security)
- Scope of computer security grew from physical security to include:
  - Safety of data
  - Limiting unauthorized access to data
  - Involvement of personnel from multiple levels of an organization
    - First identified role of management and policy

The History of Information Security

- Multics (Multiplexed Information and Computing Service)
  - Operating System
  - Security primary goal
  - Didn't go very far
  - Several developers created Unix :*Unix is a family of multitasking, multiuser computer operating systems that derive from the original AT&T Unix,*
- Late 1970s: microprocessor expanded computing capabilities and security threats
  - From mainframe to PC
  - Decentralized computing
  - Need for sharing resources increased
  - Major changed computing

The 1990s

- Networks of computers became more common; so too did the need to interconnect networks
- Internet became first manifestation of a global network of networks
- In early Internet deployments, security was treated as a low priority
  - Many of the problems that plague e-mail on the Internet are the result to this early lack of security

The Present

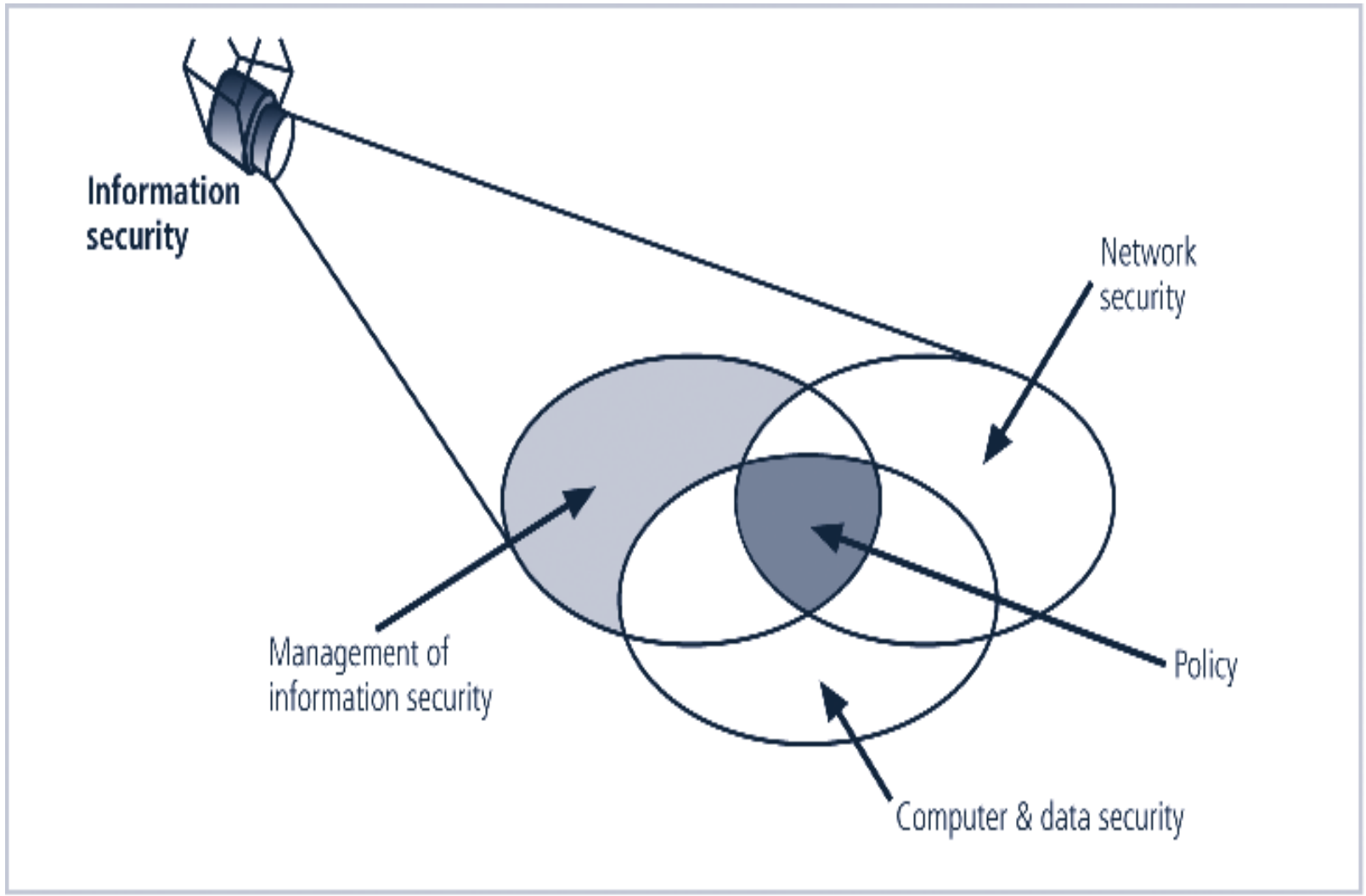
- The Internet brings millions of computer networks into communication with each other—many of them unsecured
- Ability to secure a computer's data influenced by the security of every computer to which it is connected

What is Security?

- “The quality or state of being secure—to be free from danger”
- A successful organization should have multiple layers of security in place:
  - Physical security
  - Personal security
  - Operations security
  - Communications security
  - Network security
  - Information security

What is Information Security?

- The protection of information and its critical elements, including systems and hardware that use, store, and transmit that information
- Necessary tools: policy, awareness, training, education, technology
- C.I.A. triangle was standard based on confidentiality, integrity, and availability
- C.I.A. triangle now expanded into list of critical characteristics of information



Components of Information Security

Critical Characteristics of Information

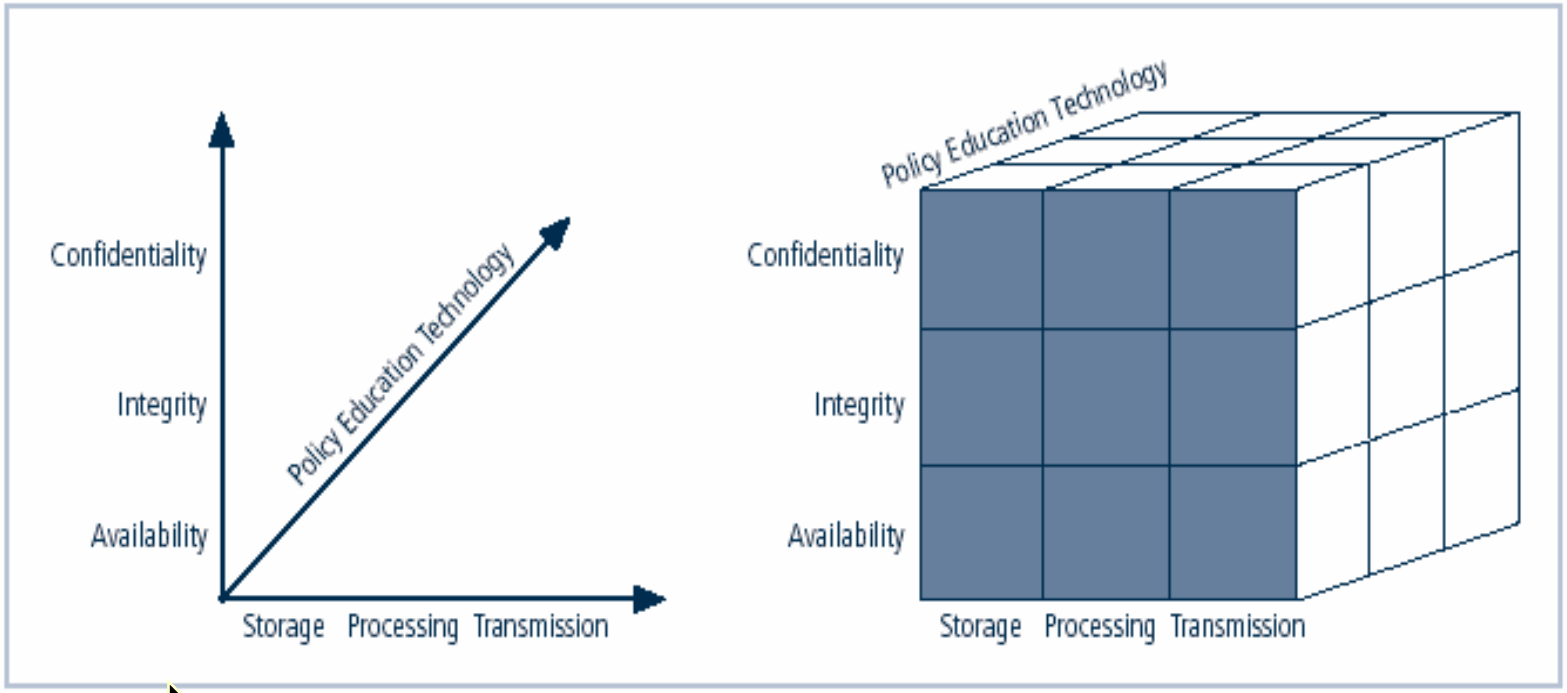
- The value of information comes from the characteristics it possesses:
  - Timeliness
    - No value if it is too late
  - Availability
    - No interference or obstruction
    - Required format
  - Accuracy
    - Free from mistakes
  - Authenticity
    - Quality or state of being genuine, i.e., sender of an email
  - Confidentiality
    - Disclosure or exposure to unauthorized individuals or system is prevented

Critical Characteristics of Information

- Integrity
  - Whole, completed, uncorrupted
  - Cornerstone
  - Size of the file, hash values, error-correcting codes, retransmission
- Utility
  - Having value for some purpose
- Possession
  - Ownership
  - Breach of confidentiality results in the breach of possession, not the reverse

NSTISSC Security Model

National Security Telecommunications & Information systems security committee



NSTISSC Security Model

Components of an Information System

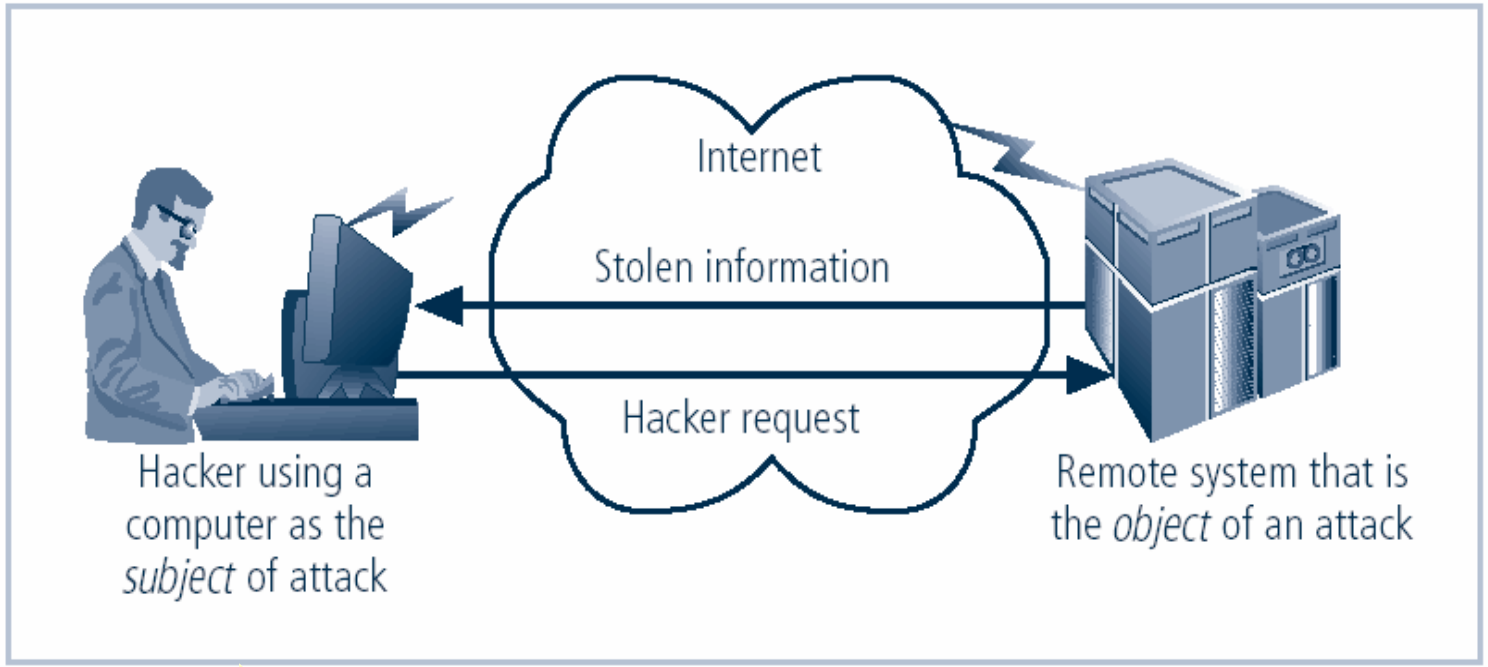
- Information System (IS) is entire set of software, hardware, data, people, procedures, and networks necessary to use information as a resource in the organization
- Software
  - Perhaps most difficult to secure
  - Easy target
  - Exploitation substantial portion of attacks on information
- Hardware
  - Physical security policies
  - Securing physical location important
  - Laptops
  - Flash memory

Components of an Information System

- Data
  - Often most valuable asset
  - Main target of intentional attacks
- People
  - Weakest link
  - Social engineering
  - Must be well trained and informed
- Procedures
  - Threat to integrity of data
- Networks
  - Locks and keys won't work

Securing Components

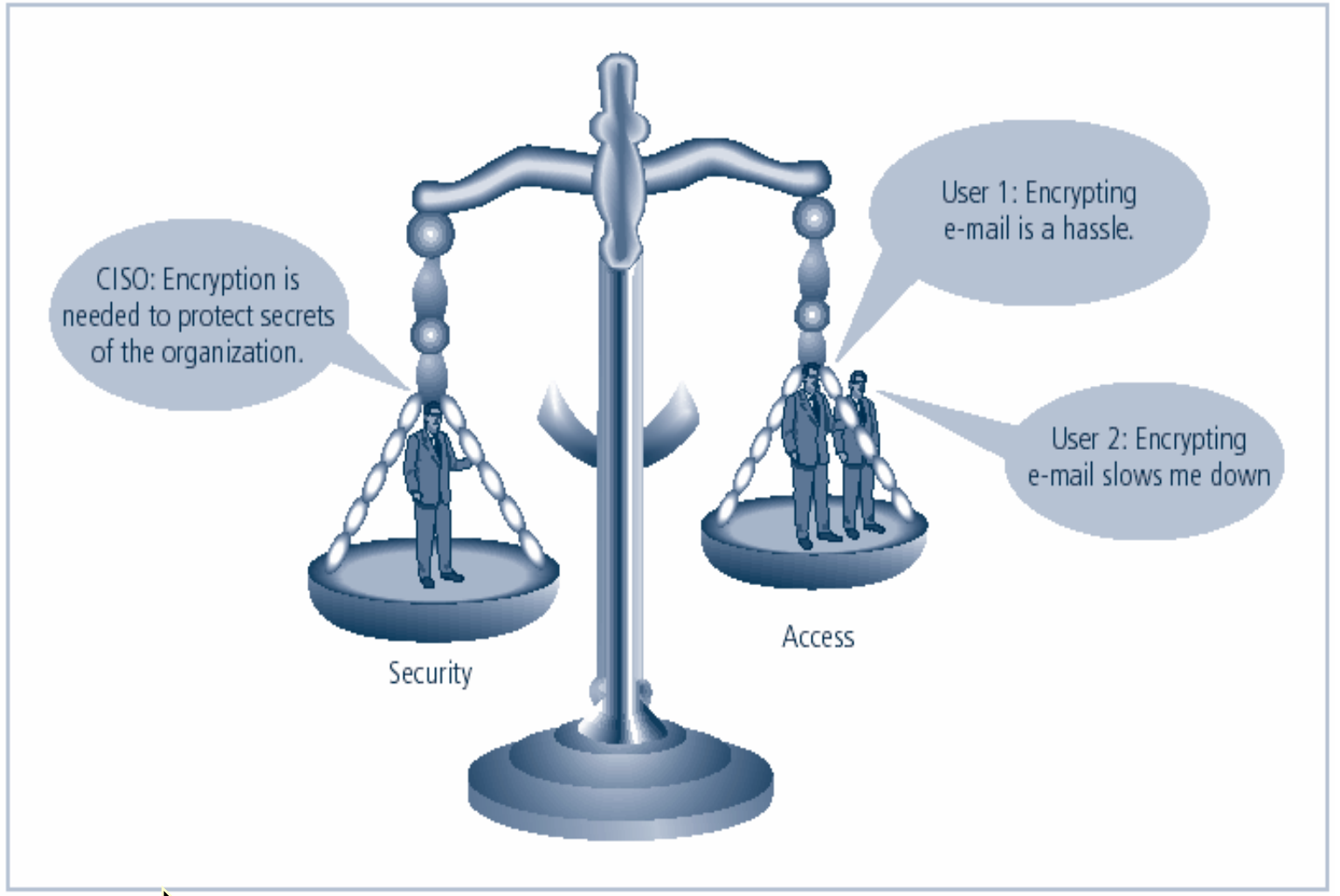
- Computer can be subject of an attack and/or the object of an attack
  - When the subject of an attack, computer is used as an active tool to conduct attack
  - When the object of an attack, computer is the entity being attacked
- 2 types of attack
  - Direct
    - Hacker uses their computer to break into a system
  - Indirect
    - System is compromised and used to attack other systems



Computer as the Subject and Object of an Attack

Balancing Information Security and Access

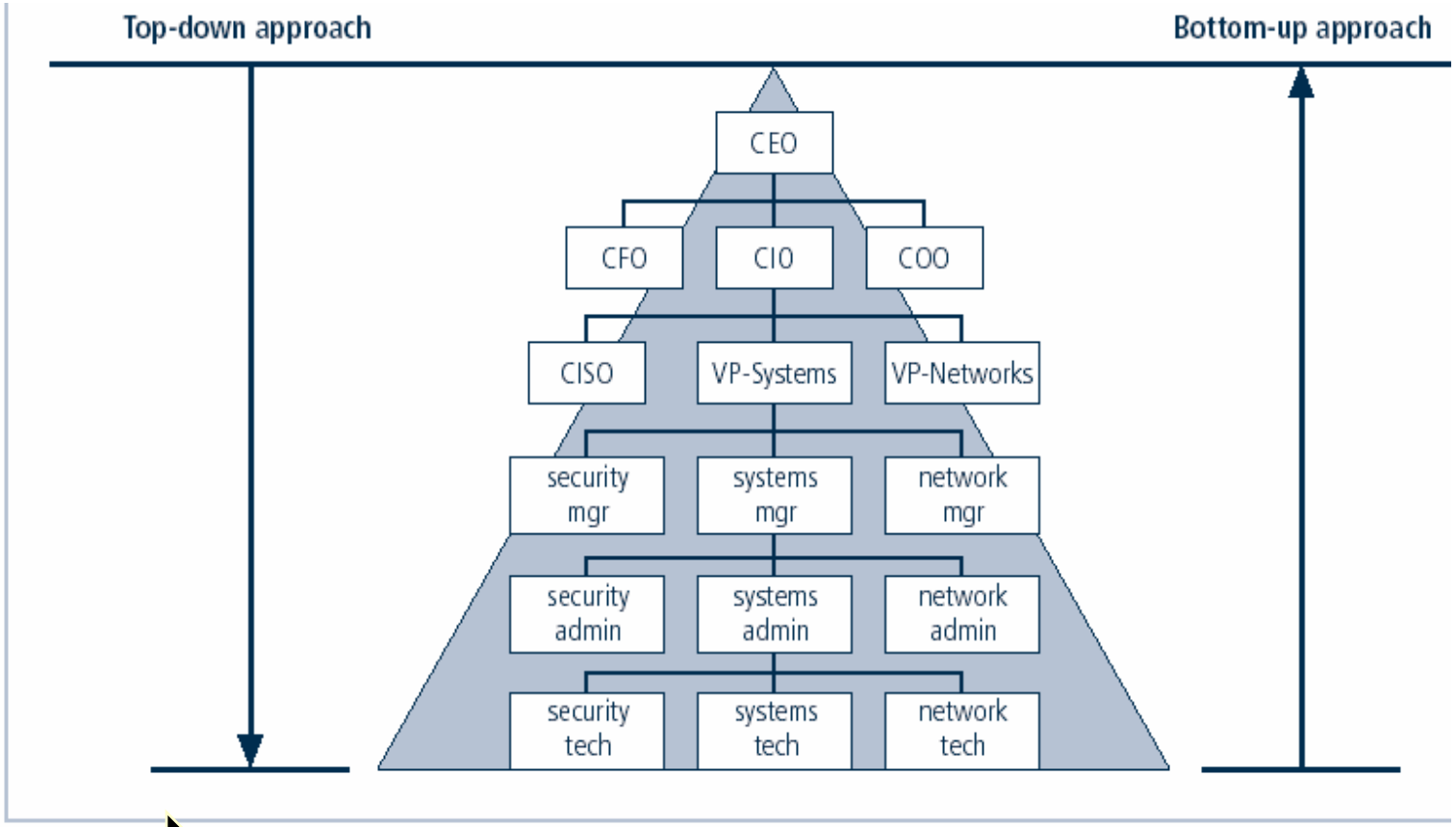
- Impossible to obtain perfect security—it is a process, not an absolute
- Security should be considered balance between protection and availability
- To achieve balance, level of security must allow reasonable access, yet protect against threats



Balancing Information Security and Access

Approaches to Information Security Implementation: Bottom-Up Approach

- Grassroots effort: systems administrators attempt to improve security of their systems
- Key advantage: technical expertise of individual administrators
- Seldom works, as it lacks a number of critical features:
  - Participant support
  - Organizational staying power



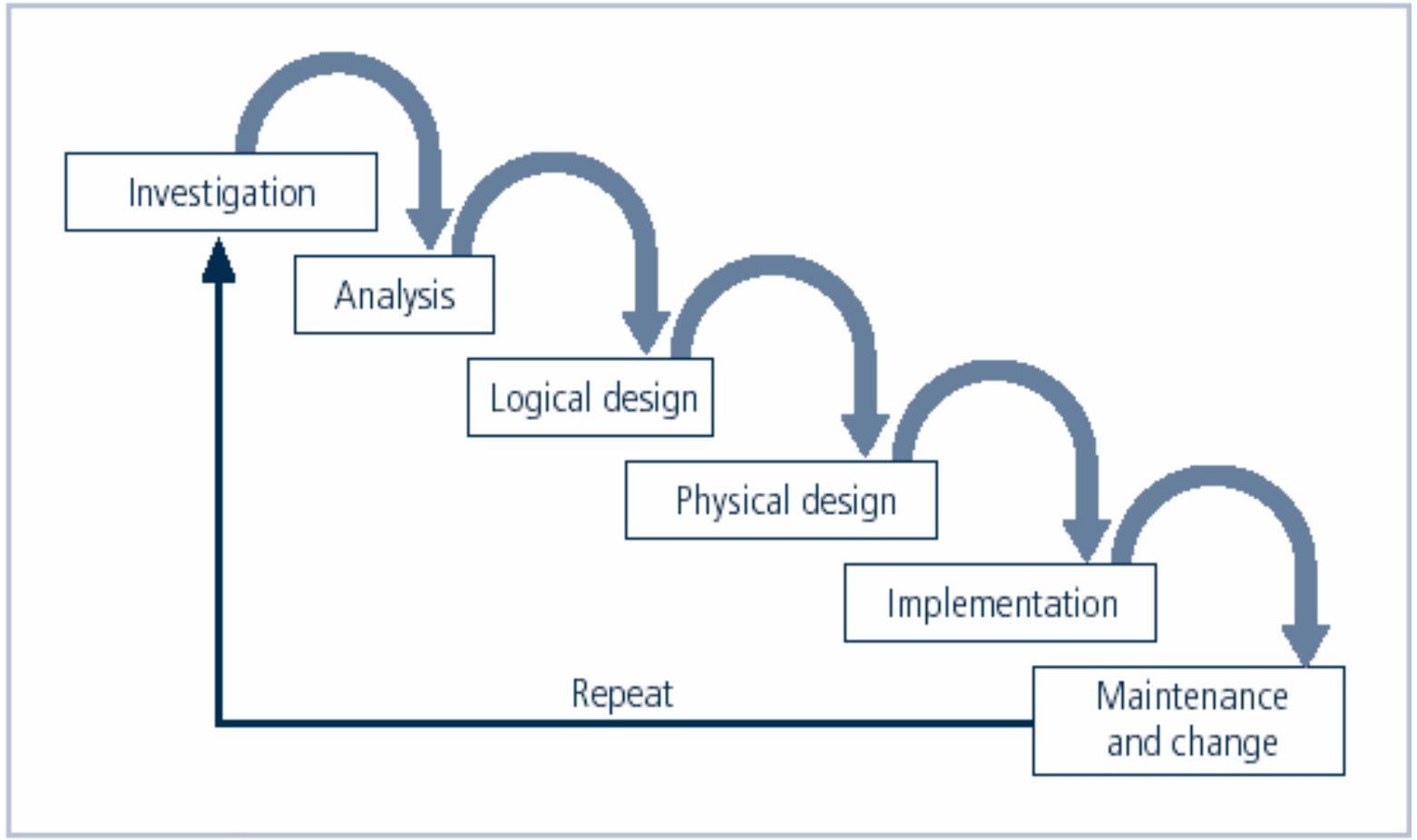
Approaches to Information Security Implementation

Approaches to Information Security Implementation: Top-Down Approach

- Initiated by upper management
  - Issue policy, procedures and processes
  - Dictate goals and expected outcomes of project
  - Determine accountability for each required action
- The most successful also involve formal development strategy referred to as systems development life cycle

The Systems Development Life Cycle

- Systems development life cycle (SDLC) is methodology and design for implementation of information security within an organization
- Methodology is formal approach to problem-solving based on structured sequence of procedures
- Using a methodology
  - ensures a rigorous process
  - avoids missing steps
- Goal is creating a comprehensive security posture/program
- Traditional SDLC consists of six general phases



SDLC Waterfall Methodology

The Security Systems Development Life Cycle

- The same phases used in traditional SDLC may be adapted to support specialized implementation of an IS project
- Identification of specific threats and creating controls to counter them
- SecSDLC is a coherent program rather than a series of random, seemingly unconnected actions

The Security Systems Development Life Cycle

- Investigation
  - Identifies process, outcomes, goals, and constraints of the project
  - Begins with enterprise information security policy
- Analysis
  - Existing security policies, legal issues,
  - Perform risk analysis

The Security Systems Development Life Cycle

- Logical Design
  - Creates and develops blueprints for information security
  - Incident response actions: Continuity planning, Incident response, Disaster recovery
  - Feasibility analysis to determine whether project should continue or be outsourced
- Physical Design
  - Needed security technology is evaluated, alternatives generated, and final design selected

The Security Systems Development Life Cycle

- Implementation
  - Security solutions are acquired, tested, implemented, and tested again
  - Personnel issues evaluated; specific training and education programs conducted
  - Entire tested package is presented to management for final approval
- Maintenance and Change
  - Most important
  - Constant changing threats
  - Constant monitoring, testing updating and implementing change

2) Videos: Discussion & Reflection

- Pause, Think and Act
- Why is Information Security Important?

- Go to the virtual room, and complete the activity thread.

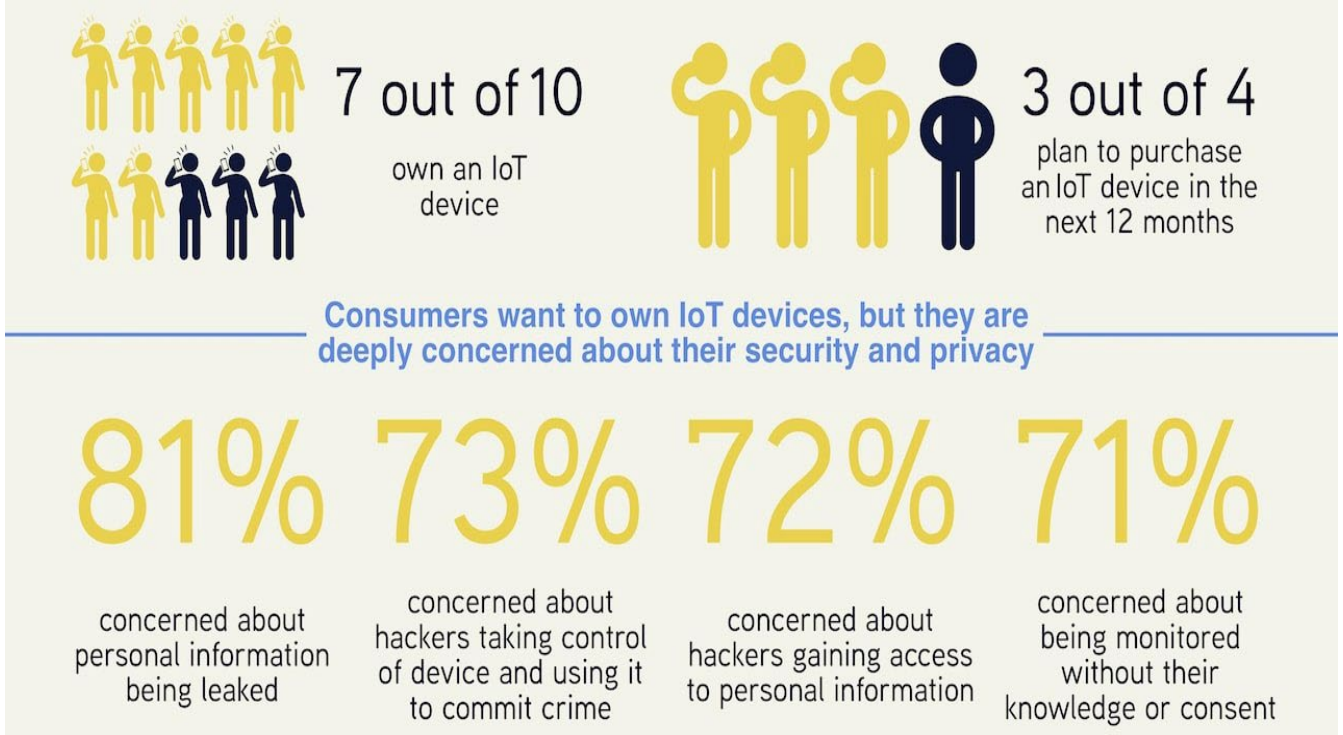
3) First Lab

Virtual | Lab

Please go to the Virtual Room for Instructions\\

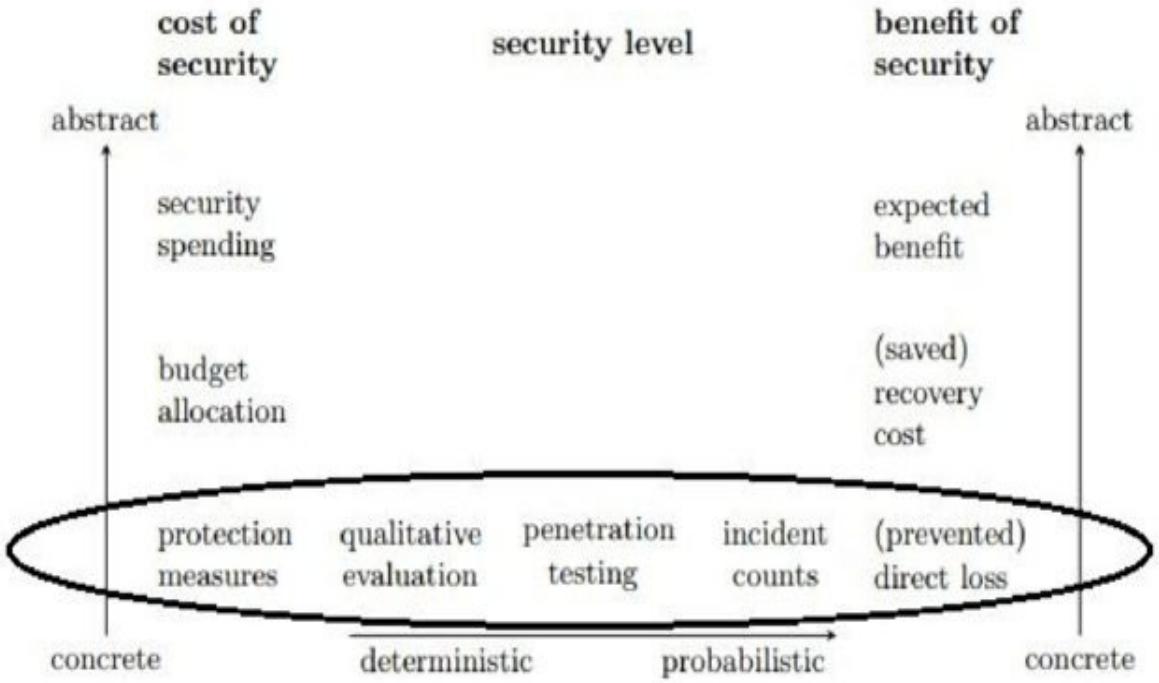
4) The Need for Security

- Information security performs four functions for an organization:
- Protects the ability to function
- Enables safe operations
- Protects data collected
- Safeguards technology assets



Protecting the Ability to Function

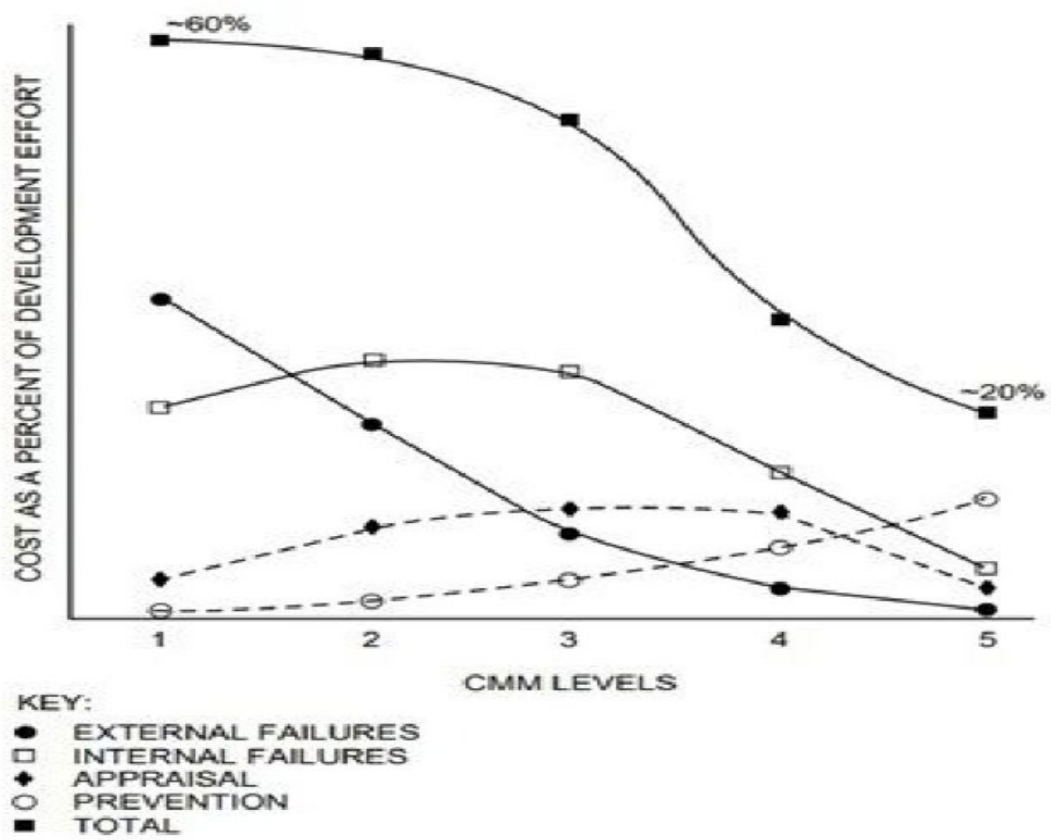
- Management is responsible
- Information security is
  - a management issue
  - a people issue
- Communities of interest must argue for information security in terms of impact and cost



Quality costs within cost/benefit relationships in information security. Adapted from Böhme (2010).

Enabling Safe Operation

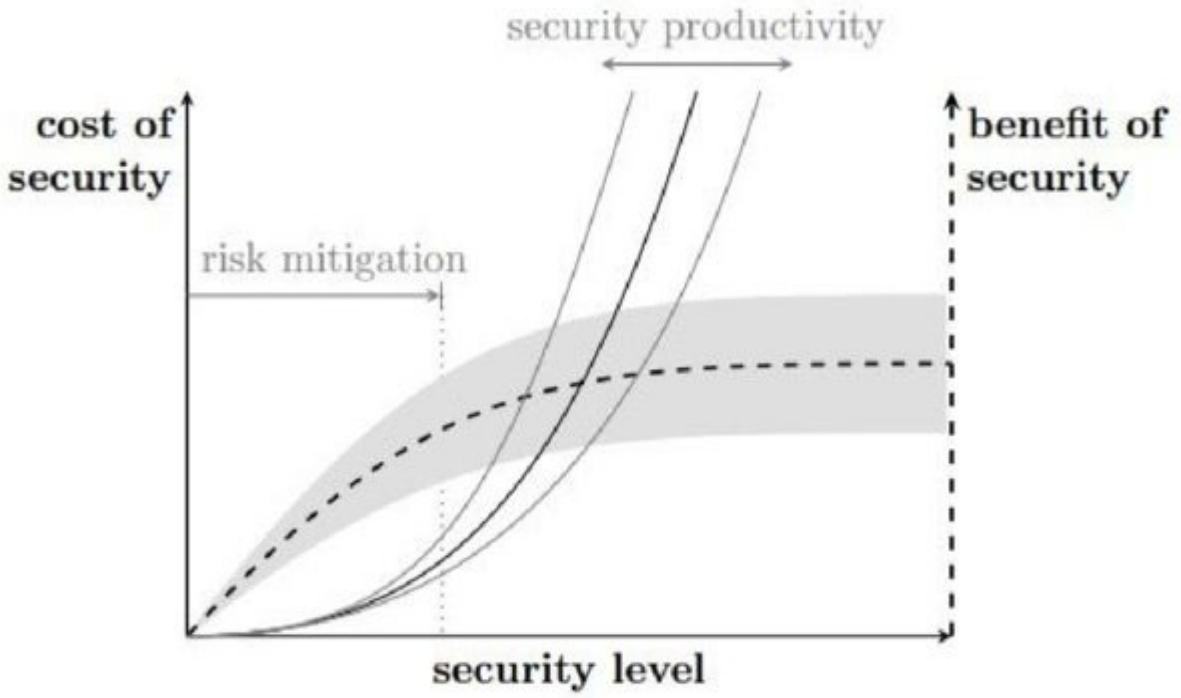
- Organizations must create integrated, efficient, and capable applications
- Organization need environments that safeguard applications
- Management must not abdicate to the IT department its responsibility to make choices and enforce decisions



Quality costs classified by organizational maturity (CMM 1=low, CMM 5=high). From Knox (1993)
CMM –Cybersecurity Capability Maturity Model

Protecting Data

- One of the most valuable assets is data
- Without data, an organization loses its record of transactions and/or its ability to deliver value to its customers
- An effective information security program is essential to the protection of the integrity and value of the organization's data



Cost/benefit relationships in information security. From Böhme (2010).

Safeguarding Technology Assets

- Organizations must have secure infrastructure services based on the size and scope of the enterprise
- Additional security services may have to be provided
- More robust solutions may be needed to replace security programs the organization has outgrown

Safeguard: *a measure taken to protect someone or something or to prevent something undesirable.*

Threats

- Management must be informed of the various kinds of threats facing the organization
- A threat is an object, person, or other entity that represents a constant danger to an asset
- By examining each threat category in turn, management effectively protects its information through policy, education and training, and technology controls

Threats to Information Security[4]

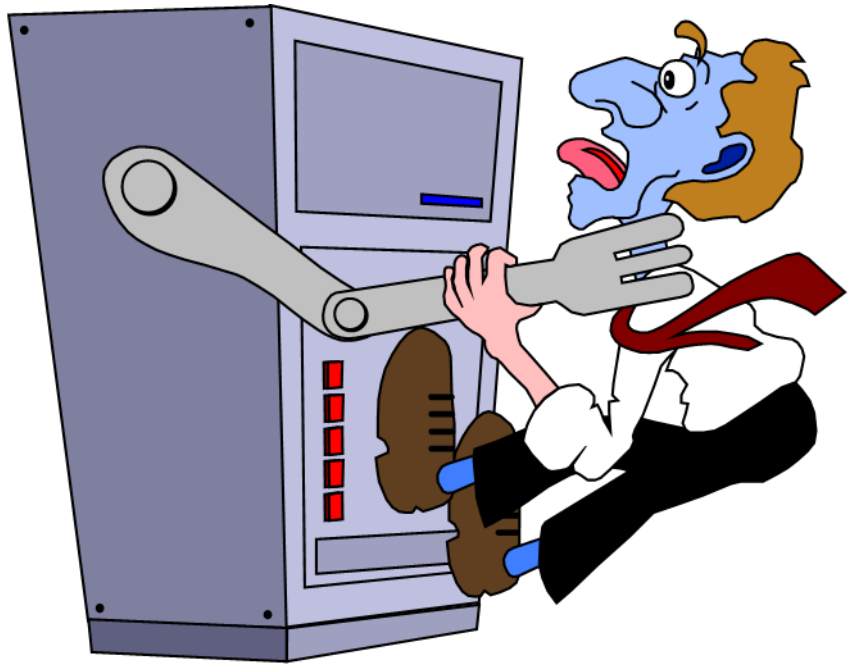
Categories of threat	Examples
1. Acts of human error or failure	Accidents, employee mistakes
2. Compromises to intellectual property	Piracy, copyright infringement
3. Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
4. Deliberate acts of information extortion	Blackmail of information disclosure
5. Deliberate acts of sabotage or vandalism	Destruction of systems or information
6. Deliberate acts of theft	Illegal confiscation of equipment or information
7. Deliberate software attacks	Viruses, worms, macros, denial-of-service
8. Forces of nature	Fire, flood, earthquake, lightning
9. Deviations in quality of service from service providers	Power and WAN service issues
10. Technical hardware failures or errors	Equipment failure
11. Technical software failures or errors	Bugs, code problems, unknown loopholes
12. Technological obsolescence	Antiquated or outdated technologies

Acts of Human Error or Failure

- Includes acts done without malicious intent
- Caused by:
  - Inexperience
  - Improper training
  - Incorrect assumptions
  - Other circumstances
- Employees are greatest threats to information security – They are closest to the organizational data

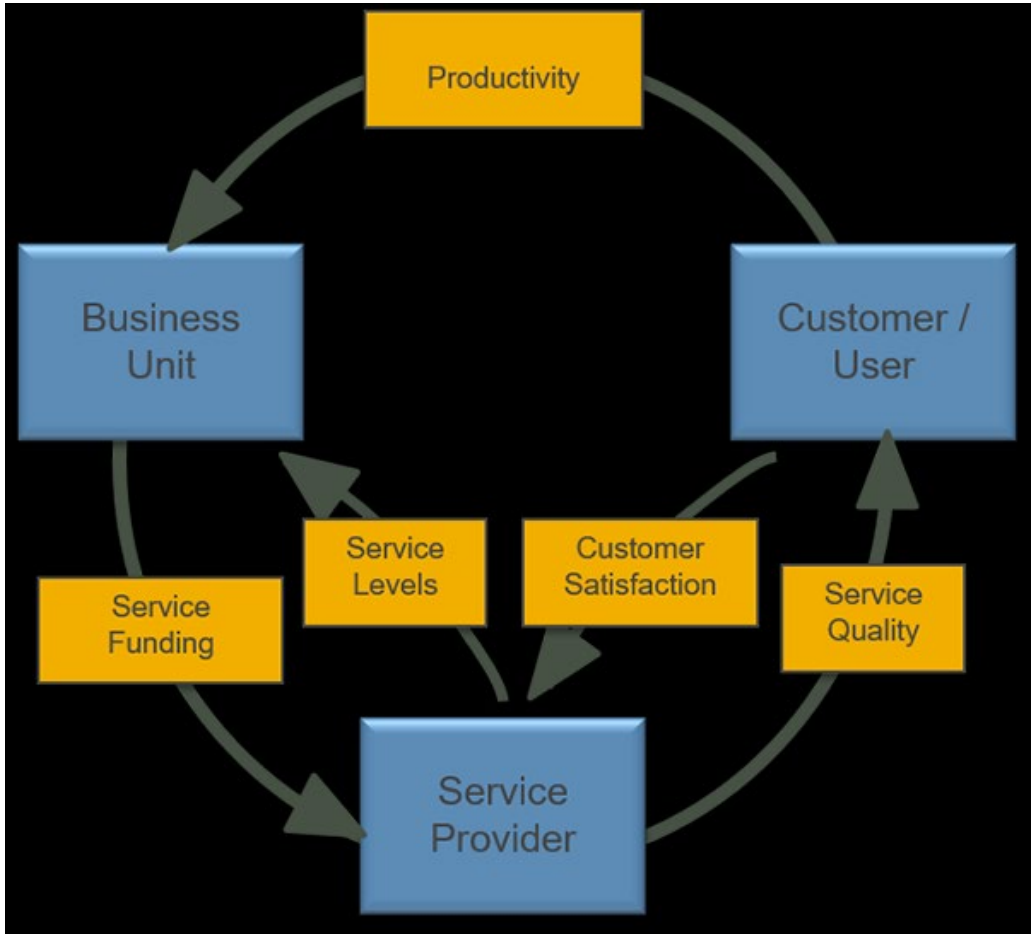
Acts of Human Error or Failure

- Employee mistakes can easily lead to the following:
  - revelation of classified data
  - entry of erroneous data
  - accidental deletion or modification of data
  - storage of data in unprotected areas
  - failure to protect information
- Many of these threats can be prevented with controls



Deviations in Quality of Service by Service Providers

- Situations of product or services not delivered as expected
- Information system depends on many inter-dependent support systems
- Three sets of service issues that dramatically affect the availability of information and systems are
  - Internet service
  - Communications
  - Power irregularities

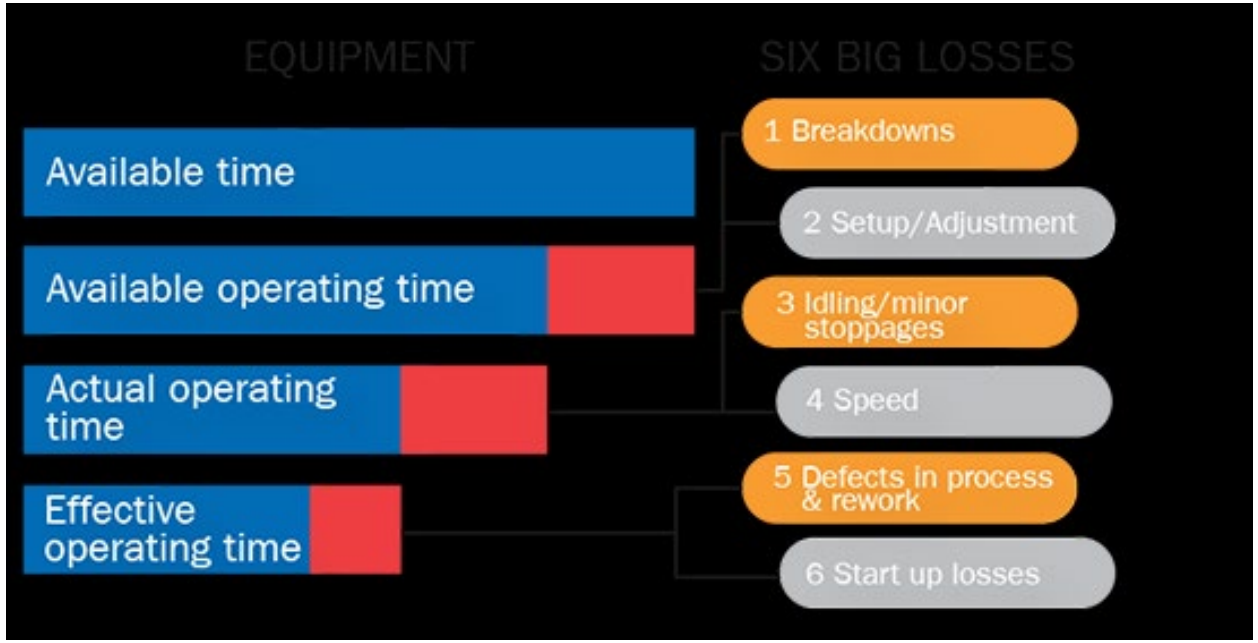


Internet Service Issues

- Loss of Internet service can lead to considerable loss in the availability of information
  - organizations have sales staff and telecommuters working at remote locations
- When an organization outsources its web servers, the outsourcer assumes responsibility for
  - All Internet Services
  - The hardware and operating system software used to operate the web site

Communications and Other Services

- Other utility services have potential impact
- Among these are
  - telephone
  - water & wastewater
  - trash pickup
  - cable television
  - natural or propane gas
  - custodial services



- The threat of loss of services can lead to inability to function properly

Power Irregularities

Voltage levels can increase, decrease, or cease:

- spike – momentary increase
- surge – prolonged increase
- sag – momentary low voltage
- brownout – prolonged drop
- fault – momentary loss of power
- blackout – prolonged loss

Overall Equipment Effectiveness	Recommended Six Big Losses	Traditional Six Big Losses
Availability Loss	Unplanned Stops	Equipment Failure
	Planned Stops	Setup and Adjustments
Performance Loss	Small Stops	Idling and Minor Stops
	Slow Cycles	Reduced Speed
Quality Loss	Production Rejects	Process Defects
	Startup Rejects	Reduced Yield
OEE	Fully Productive Time	Valuable Operating Time

OEE= Overall Equipment Effectiveness

- Electronic equipment is susceptible to fluctuations, controls can be applied to manage power quality

Espionage/Trespass

- Broad category of activities that breach confidentiality
  - Unauthorized accessing of information
  - Competitive intelligence vs. espionage
  - Shoulder surfing can occur any place a person is accessing confidential information
- Controls implemented to mark the boundaries of an organization's virtual territory giving notice to trespassers that they are encroaching on the organization's cyberspace
- Hackers uses skill, guile, or fraud to steal the property of someone else

Deliberate Acts of Theft

- Illegal taking of another's property - physical, electronic, or intellectual
- The value of information suffers when it is copied and taken away without the owner's knowledge
- Physical theft can be controlled - a wide variety of measures used from locked doors to guards or alarm systems
- Electronic theft is a more complex problem to manage and control - organizations may not even know it has occurred

What is then Cybersecurity, according to…?

- Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. – Kaspersky
- Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. – Cisco
- Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information. US Homeland Security

A new ecosystem

5) In Closing: Debriefings for Cases

- Debriefing for Cases 01 – 02 – 03 – 04
- Please go to the *Virtual Room* for Instructions
- Prepare your answers accordingly!

Thank you

Day 01

CLOSED
FOR BUSINESS

SMT
School of Management and Technology
Business School des SCMT

SCMT
Steinbeis Center of Management and Technology
Research | Education | Consulting

Steinbeis University Berlin SHB