Table of Contents

I. IT Security: Controls (072213-080213)

A. Importance of Security

Lecture Notes

- The main purpose of computer operations is to ensure that the organization is provided with information that is **Accurate, Relevant, Timely, Reliable and Sufficient (ARTR-S)**
- However, the achievement of those objectives are hampered by numerous threats such as
  - System failure
  - Poor system design
  - Insufficient and/or inaccurate data
  - Tampering of data (data diddling)
  - Viruses, worms, Trojan horses (man-made)
  - Hackers & crackers
  - Fire, smoke, earthquake
  - Fraud (e.g. embezzlement) (man-made)
  - Internal/external sabotage
- In short: "Acts of God & Acts of Man"
- Hence, IT security is *essential* to counter threats:
  - Human Error
  - Environment
  - Computer System Failure
  - Computer Crime

Notes

- *All these components (Accurate, Relevant, Timely, Reliable and Sufficient) are essential as far as operations is concerned*
- *Security is very important because there are a number of threats*
- *Threats: not man-made / not caused by people, because of* ***hardware/system failure – quality of the hardware itself***
- *Man-made threats: viruses, worms, Trojan horses*
  - ***Virus****-spreads with the aid of human action, attaches itself onto programs and files*
  - ***Worm****-spreads without the aid of human action, replicates itself*
  - ***Trojan horses****-may appear to be useful software but actually contains malicious, can cause serious damage*
- *Even if you have the most invulnerable, strongest IT security in place, it does not guarantee that you will not be hacked*
- *Lax and complacency that IT security is invulnerable → hacked!*

B. Types of Threats

1. Unintentional

a. Human Errors

Lecture Notes

- Contribute to vast majority (about 55%) of security-related problems
- Examples
  - Erroneous data entry
  - Flawed system design

Notes

- *Human errors comprise the majority of errors in systems 55%*
- *Minimize manual processing of systems → minimize human errors*

b. Computer systems failures

Lecture Notes

- Example
  - Defective materials
  - Poor manufacturing
  - CPU, Storage devices, peripheral devices, networking equipment

Notes

-

c. Environmental Hazards

Lecture Notes

- Example
  - Utilities
    - Air-conditioning
    - Power
    - Water-cooling system
  - Fire
  - Water
  - Earthquake
  - Tornadoes
  - Extreme temperatures
  - Man-made catastrophes
    - Explosion
    - Radioactive fallout

Notes

- *Some are not applicable in the Philippines e.g. tornadoes*
- *Man-made catastrophes: terrorist attacks!*

2. Intentional = Computer Crime

a. Computer as *target* of the crime

Lecture Notes

- Example: The actual hardware may be stolen or destroyed

Notes

- *Computer crime **targets** the computer*
- *E.g. hardware is the one*

targeted to be destroyed

b. Computer as *medium* or *tool* of attack

Lecture Notes

- Example: Computer may be used to **embezzle money**

Notes

- *Medium or tool of attack, not the actual target but used as a medium*
- *E.g. Hindi target yung actual hardware, walang ginagawang masama sa computer*
- *Used to attack the system itself*

c. Computer can be used to *intimidate* or *deceive*

Lecture Notes

- Example: Stockbroker stole money by convincing clients of a software which will increase ROI by 60% per month

Notes

- *A system has been developed by the one who wants to deceive, usually a software.*
- *Software gives false information or data to the one that he/she wants to deceive*
- *Used to deceive a person or group of people*

C. Defense Strategy & Its Objectives

Lecture Notes

- Selection of a specific defense strategy depends on objective of defense & perceived cost-benefit
  - Prevention & Deterrence

Notes

- *Incorporate most, if not all, of the objectives*
- *Prevention: not allowing that threat to happen, completely preventing it, not allowing it to happen*
  - *Preventive maintenance, ayaw mo mangyari*
- *Deterrence: discourage from doing something*
- *Example: car is being stolen. Preventive measure vs deterrence measure*
  - ***Preventive: Anti-theft system***
  - ***Deterrence: red light that blinks, deter you from stealing the car ("panakot***

	lang”)
○ Detection	- *Threat is* ***already happening*** - *E.g. suspicious (monitoring their movements), when they break in, detection → report agad,, censors in place (detects)*
○ Limitation of Damage	- *Implies that the* ***threat happened already****,* ***minimize the damage*** *caused by the actual threat; don’t let it spread*
○ Recovery	- *After the damage, you should be able to* ***restore the previous state of the system***
○ Correction	- *Something is wrong with the security system, correct that to prevent from happening again*
○ Awareness & Compliance	- ***Document*** *the security protocols, spreading the documentation, comply with them*

D. Controls

Lecture Notes	***Notes***
- Provide means of protecting IT	-
- Integrated during systems development	
- Implemented once system is in operation	
- Meant to protect all components of the system:	
○ Hardware	
○ Software	
○ Data	
○ Network	

1. Challenge of Controls

Lecture Notes	***Notes***
- **To balance**: the need of the organization for information to assist in decision making	- *Assist and protect*
- **With**: The need to protect this information to ensure that it meet the organization’s requirements	

2. Characteristics of Good Controls

a. Complete

Lecture Notes	***Notes***
-	-

b. Effective

Lecture Notes	Notes
-	-

c. Timely

Lecture Notes	Notes
-	-

3. Major Categories of Controls

a. General Controls

Lecture Notes	Notes
- Established to protect the system regardless of the specific application	-

i. Physical Controls

Lecture Notes	Notes
- Protection of computer facilities & resources - Prevention of physical damage due to natural & unnatural disasters such as o Earthquakes o Floods o Fire o Physical attack on the computer	-

a. Against Fire

Lecture Notes	Notes
- Sprinkler system - Use of gas-based fire suppressants	-

b. Against Power Outages

Lecture Notes	Notes
- Use of uninterruptible power supply (UPS) preferably intelligent ones for servers	-

c. Against lightning & other induced currents

Lecture Notes	Notes
- Lightning rods - Surge protection for both power & network cables - Metal conduits for UTP cables especially those close to fluorescent lighting units & those located outside	-

ii. Access Controls

Lecture Notes	Notes
- Restriction of unauthorized user access to a portion	-

of a computer system or the entire system

a. Physical Access to a terminal

Lecture Notes	**Notes**
- Use of coded key entry, swipe card, biometric controls	-

b. Logical Access to the system

i. Firewalls

Lecture Notes	**Notes**
- Allows only authorized traffic into the network	-

ii. Network

Lecture Notes	**Notes**
- Require network log-in (log-in name & passwords)	- *5 secs of aging*
- Password aging – password expires after some time	
- Password rotation – password must be replaced a number of times before re-using	
- Log-in control – account disabled after a number of consecutive unsuccessful log-ins	

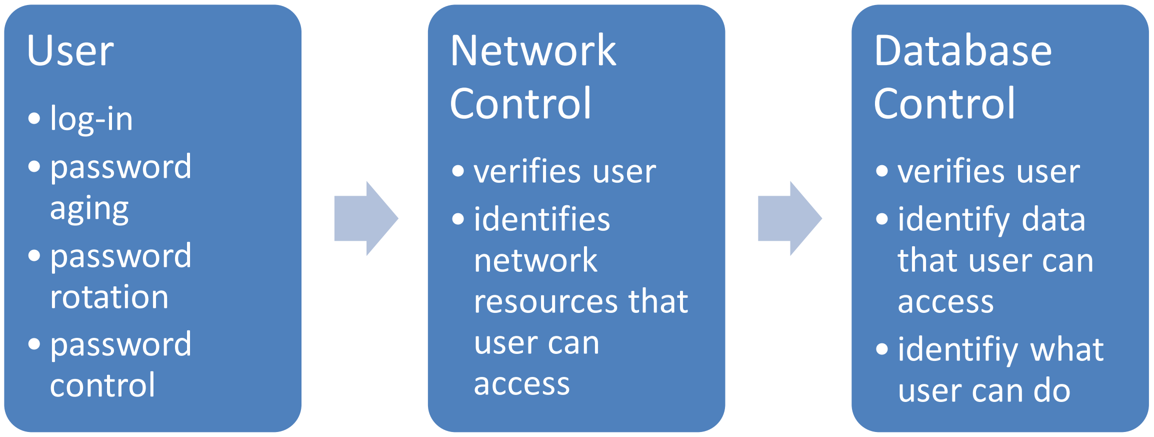
iii. Database system log-in

Lecture Notes	**Notes**
-	-

c. Access to specific system privileges

Lecture Notes	**Notes**
- Based on user's ID, limit which data can be accessed	-
- Limit what can be done with data – read, update, delete, insert	

d. Two-Level Logical Access Control



User
- log-in
- password aging
- password rotation
- password control

Network Control
- verifies user
- identifies network resources that user can access

Database Control
- verifies user
- identify data that user can access
- identifiy what user can do

Lecture Notes ***Notes***

-

-

e. Illustration of Access Controls

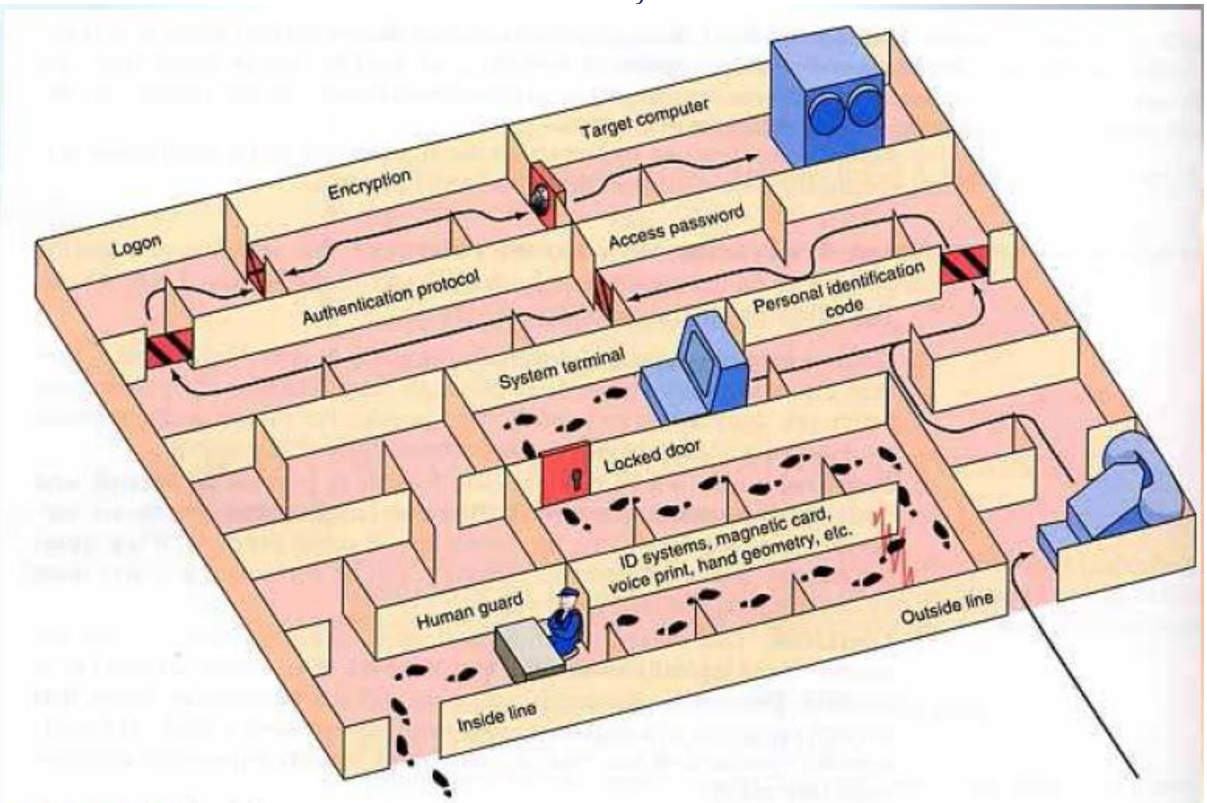


FIGURE 15.6 The defense. (*Source:* Joe Lertola.© 1983 *Discover* magazine.)

Lecture Notes	***Notes***
-	-

iii. Data Security Controls

Lecture Notes	***Notes***
- Protection of data from intentional or accidental disclosure or from unauthorized modification or destruction	- *Focus is DATA*
- Addresses the following ○ Confidentiality of data ○ Access control ○ Critical nature of data ○ Integrity of data	- *There are areas with confidential access control*

a. Minimal Privilege

Lecture Notes	***Notes***
- Ensures that only the required information is accessible to the user	- *Example: Kahit friends, may limited access* - *Accessible only what you are required to do, or what is your job* - *Facebook example*

b. Minimal Exposure

Lecture Notes	***Notes***
- Ensures that only those that require the information should obtain it	- *Segregates authorized users* - *Who can access information*

iv. Communications & Network Controls

Lecture Notes	***Notes***
- Protection of network components due to the internet & proliferation of e-commerce - Ensure that the network will continue to operate at an acceptable level	- *Will be discussed in networking*

v. Administrative Controls

Lecture Notes	***Notes***
- Deal with issuing guidelines & monitoring compliance with the guidelines	- *MOST MANUAL* - *These are guidelines & documentations*
○ Immediate revocation of access rights of **terminated or resigned employees**	- *Ex: Resigned employees, account is active in a company* ○ *THREAT: Someone else can use that account*
○ **Virus protection guidelines**	- *Administering & monitoring virus in network*

	○ *Ex: Can't use personal device*
○ **Separation of duties** – divide sensitive duties among as many as economically feasible to decrease chance of intentional/unintentional damage	- *Power corrupts* ○ *Ex: IM is one person; can borrow money / laundering*
○ Periodic audit of information systems	- *Audit: usually in banking, accounting* - *IT audit: part of accounting audit*
○ Fostering company loyalty	- *Because…can hack the system* - *Give out confidential information* - *Competitors piracy*
○ Insurance for key employees	- *Life insurance for a key employee* - *Ex: Pag namatay yung key employee (CEO dies) …* - *Succession plan* - *Learning curve of the replacement* - *Company buys life insurance and it benefits the company, usually employee buys for themselves*

vi. Programming Controls

Lecture Notes	***Notes***
- Aim to reduce errors in programming - Causes include use of incorrect algorithm, carelessness, inadequate testing & configuration management, etc. - Examples: ○ Training ○ Establishing standards for testing & configuration management ○ Enforcing documentation standards	-

vii. Documentation Controls

Lecture Notes	***Notes***
- Ensure that manuals are easy to read & understandable and always up-to-date - Appropriate documentation controls include accurate writing, standardization updating, testing,	-

etc.

- Use of CASE tools to document system
- Most common system documents
  - System standards
  - Program specification & actual code documentation
  - Data & database documentation
  - Operations manual
  - User's manual
  - Training manual
  - Conceptual, logical, & physical ERD

viii. System Development Controls

Lecture Notes

- Ensure that a system is developed according to established policies & procedures
- Conformity with budget, timing, security measures, & quality as well as documentation requirements must be maintained

Notes

- *Focuses on SDLC*
  - *Companies have customized methodologies*
  - *Has to be very specific on the deliverables and/or artifact*
  - ***Deliverable == Artifact** in a context of Object Oriented Approach (OOA)*
  - *OOA – unified process, stem from Traditional SDLC*
- *System Development controls two points: delivering the project on **time** and within **budget***
  - *20% on time and within budget*

b. Application controls

Lecture Notes

- Safeguard intended to protect specific applications
- Controls built into applications & are usually written as validation rules
- Ensure that all transactions are accurately recorded, classified, processed, and reported

Notes

-

i. Input Controls

Lecture Notes

- Designed to prevent data alterations or loss
- Very important because they prevent "garbage-in, garbage-out" situations

Notes

-

a. Recording of transactions

i. Manual Forms

Lecture Notes

- Use well-structured, pre-numbered source documents
- Provide space for necessary authorizations
- Ensure blank forms are controlled & kept safe, preferably under lock & key

Notes

- *Examples: Land titles, letterhead*

ii. Online Forms

Lecture Notes

- Use pre-formatted, menu-driven screens
- Use standard readers (e.g. bar-code) to reduce input errors
- Provide feedback mechanisms to approve transactions

Notes

- *Instead of keyboard entry, standard readers*
    - *Minimizes errors on input*
- *Provide feedback mechanism to approve transactions*

b. Batching of transactions

Lecture Notes

- Batch control totals help prevent data loss & erroneous posting of transactions
- Use of batch control logs for batch number & totals

Notes

- *Deals with batch programs; are executed on a non-real time basis*

i. Amount control totals

Lecture Notes

-

Notes

- *Deal with money, non-monetary fields that makes sense to add them all up*

ii. Hash totals

Lecture Notes

-

Notes

- *CHKSUM*
- *What fields do you normally use Hash totals?*
- *Example: student ID number, numeric but does not make sense to add them*
- *Monitoring a specific batch if they are added or not in a specific batch*

iii. Record count

Lecture Notes

Notes

-	- *Number of records, rows within a specific group,, or batch of records*

c. Conversion of transaction data

Lecture Notes	***Notes***
- Data conversion by keying, scanning, or copying from one source document to another	- *Conversion plans* - *Convert data from one system to another, there are many possibilities. Those are paper-based • electronic form (encoding) • prone to error 55% of errors*
- All converted data must be verified either visually or by key verification	- *Scanner's with* ***OCR (Optical Character Recognition)*** - *A verification will show to check if the scan / recognition is correct*

d. Editing of transaction data

Lecture Notes	***Notes***
- Use of edit tests (program validation routines) to compare incoming data with a standard	-

i. Self-checking digit (check digit)

Lecture Notes	***Notes***
-	- *16579 – 0* - *Check digit is used for editing* - *Computed based on what has been inputted* - *Get the total, divide by 5 and get the modulo* - *How do you take care of that?* ○ *Multiple by the weights… (listen to recording)* ○ *Transposition*

ii. Range check

Lecture Notes	***Notes***
-	- *DOMAIN* - *Allowable values for a specific column* - *It applies to numbers, characters; it applies to allowable values for a specific*

field or column

iii. *Limit check or reasonableness check*

Lecture Notes	**Notes**
-	- *It's more complex than range* - *Combination of several conditions* ○ *HR system, merong napromote, tapos nagincrease yung sweldo, yung increase nya 500%, yung prinomote kakapasok pa lang. the performance of that person is questionable. Based on those several conditions.* ○ *Is it reasonable?* - *Based on several conditions*

iv. *Format or data type check*

Lecture Notes	**Notes**
-	- *If it's a number, you can only put in numbers.* - *Telephone number – may specific format yun, the same for international number, may standard* - *Name – First name, Middle Initial, Last name, ID number – 6 digit number; hindi ka pwede maglagay ng characters*

v. *Dependency or relationship check*

Lecture Notes	**Notes**
-	- *Foreign and primary key*

e. *Transmission of transaction data*

Lecture Notes	**Notes**
- When data must be transmitted from point of origin to the processing center through data communications facilities, the following must be considered	- *Checks the integrity of the transmitted data from the…*

i. *Echo check*

Lecture Notes	**Notes**
-	- *The data gets garbled along the*

way, when it transmits to the server, iba na. it sends data to the server tapos bago icommit yung transaction, it echoes the data back to the client and the client verifies the data if tama. The user checks if tama then tsaka palang magcommit

ii. *Redundancy data check*

Lecture Notes	***Notes***
-	- Captcha: type this if you're human. What's the purpose? ○ **Prove if you're human:** Reduce spammers – bots; what are bots? Bakit bot? Short for robot. Kasi automated yun that spam accounts. It's highly improbable that bots can figure out the garbled letters in captcha. When an OCR (optical character reader) tries to figure what the letters are, it might make a mistake ○ **Helping in trying to figure out what those scanned phrases are.** Yung isa known yung isa unknown (two phrases, yung isa dun). One purpose is trying to help them or identify what those terms are.

iii. *Completeness check*

Lecture Notes	***Notes***
-	- *Example: Gmail's password & username*

ii. Processing Controls

Lecture Notes	***Notes***
- Ensure that data are complete, valid, & accurate when being processed & that programs have been	-

properly executed

a. *Manual cross-checks*

Lecture Notes	**Notes**
-	- *Cross-checking* - *When you're processing data, what do you do?* - *You verify whether the transactions processed using several documents* - *Tama ba to? Does it match with this particular document*

b. *Processing logic checks*

Lecture Notes	**Notes**
-	- *Edit tests which can be done during processing (slide editing of transaction data)* - *Are done during editing or input*

c. *Run-to-run totals*

Lecture Notes	**Notes**
-	- *Record count* - *Hash totals* - *Done during input* - *Input (batching of transaction data slide)* - *They make sure there are no inserted or deleted data after processing has been completed* - *Tama ba yung number na pinrocess nya?*

d. *File & program changes*

Lecture Notes	**Notes**
-	- *Essentially affect where transactions are posted on* - *Master files – very very important* - *You make sure if there are file and program changes that have been made in the system.* - *Make sure the transactions are posted where they should be posted* - ***Regression testing***

- *Stress test, system test*
- *You've already completed the test plan, and the system has already been implemented in production.*
- *You have revised, and you need to repeat those tests. You regress to make sure they are still unaffected. Important if you have made important revisions to the system.*

e. *Audit trail linkages*

Lecture Notes	***Notes***
-	- *What's an audit trail?* - *Log of all activities in the system* - *Sino nakalog in, ano ginawwa nya, kelan ginawa, etc.* - *So pag may naghack sa system, makikita kung ano ginawa system, kung sino* - *In mysql, you can track sino yung mga nakalog* - *If you want to capture everything as to capturing less information, what do you have to balance? Storage. If you capture everything and store all of them, that would create a very very large lob file. If you capture less information, it creates a smaller file. You compromise information.*

iii. Output Controls

Lecture Notes	***Notes***
- Ensure that the results of computer processing are accurate, valid, complete & consistent	-

a. *Review of processing results*

Lecture Notes	***Notes***
-	-

b. *Controlled distribution of outputs*

Lecture Notes	***Notes***

-	- Kung sino lang may kailangan makakita nun, sila lang nakakita ng report. - Based on "minimal access exposure" - Minimum privilege, makikita ka ng report, pero limited access mo dun sa access na un

II. IT Security: Business Continuity Planning

A. The Need To Be Prepared

Lecture Notes	***Notes***
- Disasters occur without warning & the best defense is **preparedness** - Advance crisis planning can help minimize losses - An important element in any security system is the **business continuity plan**	- *Important but often neglected*

B. Business Continuity Plan (BCP)

Lecture Notes	***Notes***
- **Business process contingency plan** - Purpose: to **keep critical business functions running with minimal or no interruptions after a disaster occurs** - Also outlines the process by which businesses would recover from a major disaster	-

1. Comprehensiveness of BCP

a. Total Continuity Program Management

Lecture Notes	***Notes***
- Overall project management - Crisis management - Risk management - Industry benchmark	-

b. Business Continuity Program Design

Lecture Notes	***Notes***

- Understand business & IT requirements - Evaluate current capabilities - Develop continuity plan	-

c. IT Recovery Program Design

Lecture Notes	***Notes***
- Assess IT capabilities - Develop recovery procedures - Design solutions	-

d. IT Recovery Program Execution

Lecture Notes	***Notes***
- Recovery tasks - Testing - Other functional exercise of recovery plan & procedure	-

2. Disaster Recovery Plan (DRP)

Lecture Notes	***Notes***
- Sometimes suggested to be synonymous with BCP, but the two are actually different - In the IT context, a DRP documents actions to be taken to restore computer processing, applications, telecommunications, and data after a disruption to minimize impact on business - Considered part of BCP	- *IT part of the BCP*

3. Steps in BC Planning

a. Premises

i. Business recovery planning

Lecture Notes	***Notes***
-	-

ii. Business continuity planning

Lecture Notes	***Notes***
-	-

iii. Business continuity policy

Lecture Notes	***Notes***
-	-

b. Initiate BCP project

Lecture Notes	***Notes***
-	- *Come with project proposal*

- *Budget approval from top management*

c. Identify business threat

Lecture Notes	***Notes***
-	- *Threat that*

d. Conduct risk analysis

Lecture Notes	***Notes***
-	- *Risks | Probability | Impact*

e. Establish business continuity plan

Lecture Notes	***Notes***
- Establish recovery team	- *Assemble team – **design & recovery team*** - *BCP – there are a lot of people in that team: scope, limitations* - *Recovery – comprised of IT people because IT component yung DRP* - *Scope is very very important*

f. Design business continuity plan

Lecture Notes	***Notes***
- Design recovery plan	- *Critical component: Design BRP*

g. Define business continuity process

Lecture Notes	***Notes***
- Define recovery process	- *Details*

h. Test business continuity plan

Lecture Notes	***Notes***
- Test recovery plan	- *Simulating a real disaster*

i. Review business continuity plan

Lecture Notes	***Notes***
- Review recovery plan	- *Identify steps that did not work*

4. Key Thoughts

Lecture Notes	***Notes***
- Ensures IS is able to recover efficiently & in the least amount of time after a disaster - Part of asset protection - Should focus first on recovery from total loss of all capabilities	- *Worst case scenario*

- Both IS & management should be involved in preparation of plan
- BCP must be **tested periodically**
- An outdated plan is worse than having no plan at all
- BCP should be well-documented & kept in a safe but accessible place
- The plan must be audited regularly
- The plan should be written so that it is effective in case of disaster & not just to satisfy auditors
- All critical applications must be identified & recovery procedures addressed
- Accompanied by management & end-users responsibilities

C. Management Responsibilities

Lecture Notes

- Determines scope of BCP
- Determines maximum amount of time for an application to be recovered
- Makes business decisions on recovery alternatives
- Accepts risks for possible exposures
- Accepts responsibility for the continuity of business until IS recovers

Notes

- *Ones who **decide***
-

D. User Responsibilities

Lecture Notes

- Provides input on selection of most critical application systems
- Provides input on maximum amount of time allowable for recovery
- Provides input to management on impact to business of application system loss, time constraints for recovery, and possible data processing

Notes

- *Front lines*
- *Provides the input*
- *Using the system, best position to provide inputs on critical applications*

E. Backup & Recovery

Lecture Notes

- Backup: one of the most logical ways to deal with data loss
- Included in BCP

Notes

- *Not just of data files*
- *There's also backup of data centers*

1. Backup of data files

Lecture Notes

Notes

- Backup critical data regularly
- Store backup media both in local (onsite) & remote sites (offsite)
- Practice recovery procedures regularly

- *Onsite: within the premises, vicinity*
- *Offsite: at least 10km*
- *Don't practice recovery procedures regularly*
    - *Archived DVD not working*

a. Types of Data File Backup (*see example*)

i. Full

Lecture Notes

- All selected files are backed-up

Notes

- *Highly dependent on the backup size*
- *Identify files, Even those files that are not changed are backed up*
- ***Disadvantage: Storage & speed***

ii. Differential

Lecture Notes

- New & changed files since last full, regardless whether file changed during last backup or not

Notes

- *Work with full backup*
- *A: Easier to restore*

iii. Incremental

Lecture Notes

- New & changed files since last backup

Notes

- *Work with full backup*
- *A: Less storage*

b. Data File Backup Schemes

i. No media rotation

Lecture Notes

- Only one tape/medium is re-used depending on backup frequency
- Does not archive history of data

Notes

- *Only one medium*

ii. With media rotation

Lecture Notes

- Reuses several media based on predetermined scheme
- Popular rotation schemes include:

Notes

- *Several media, rotate among popular schemes*

a. Round robin

Lecture Notes

- Uses five tapes (one tape per day of the workweek)
- Does not lose more than a day's worth of data

Notes

- *5 days → earliest*
- *5 media*

b. Grandfather, Father, Son (GFS)

Lecture Notes

- Most common scheme
- Daily – weekly – monthly
- Disadvantage: needs a large number of tapes

Notes

- *Up to A YEAR worth of backup*
- *More tapes*
    - *Daily tapes (4) (no record on last day, because weekly tape is used)*
    - *Weekly tapes (4/5)*
    - *Monthly tapes (12)*
- *Total: 20/21 tapes will be used*

c. Tower of Hanoi

Lecture Notes

- Based on math puzzle
- Uses full backups
- The more often a media set is used, the more recent the archived data
- Doubles backup history with every additional tape
- Best practice: 8 if daily, 5 if weekly
- Example: 5 dailies –ABACABADABACABA…
- Disadvantage: long backup window

Notes

-

2. Backup of data center

Lecture Notes

- Provides location from which recovery can take place
- This location is known as backup site
- Where the data center will be recreated and will operate from, for the length of disaster
- Useless without definitive BCP

Notes

-

a. Configuration of Backup Site

i. Hot site

ii. Warm site

iii. Cold site

b. Sources of Backup Site

i. Mutual agreement with another company

ii. Shared disaster recovery center

iii. Second data center

iv. Third-party data center

F. BCP in Action: Blue Cross

III. IT Security: Business Continuity Planning

A. Hacking: A Serious Threat

Lecture Notes	***Notes***
- Definition: Hacker o A person who enjoys exploring the details of programmable systems & how to stretch their capabilities o One who programs enthusiastically o A person who is good at programming quickly o An expert at a particular program, as in a 'a Unix hacker' o [Deprecated] A malicious meddler who tries to discover sensitive information by poking around. The correct term for this sense is "cracker"	-

B. Motivations for Hacking

1. For fun

2. As a challenge

3. As a legitimate job ("white-hat")

4. For personal gains ("black-hat"

C. Brief History of Hacking

1. Pre-1969: Operators as pranksters

Lecture Notes	***Notes***
- Pre-1969: Operators as pranksters	-

2. 1960s: Hacks (MIT) simple programming shortcuts

Lecture Notes	***Notes***
- 1960s: Hacks (MIT) were simply programming shortcuts to speed up computing task	-

3. 1969: Dennis Ritchie & Ken Thompson

Lecture Notes	***Notes***
- 1969: Dennis Ritchie and Ken Thompson	-

4. 1970s: Cap'n Crunch Cereal's giveaway whistle

Lecture Notes	***Notes***

- 1970s: Cap'n Crunch Cereal's giveaway whistle produced a 2600 MHz sound used in telephones ("phone phreaking")

-

5. 1980: Start of "Golden Age"

Lecture Notes

- 1980: Start of "Golden Age" with the introduction of IBM PC

Notes

-

6. 1984-1990: Great Hacker War

Lecture Notes

- 1984-1990: Great Hacker War
  - Legion of Doom vs. Masters of Deception

Notes

- *Advent of PC*
- *Legion of Doom*
- *Inspired by Saturday noon cartoons, Lex Luther → Phiber Optik, teenage cocky*
- *Erik Bloodaxe vs Phiber Optik*
- *Phiber Optik kicked out → formed Masters of Deception*

7. 1986: Federal Computer Fraud & Abuse Act

Lecture Notes

- 1986: Federal Computer Fraud & Abuse Act
  - Led to arrest & time served for many hackers
  - Initially, not punitive enough ($10,000 fine and community service, a year in prison, etc.)

Notes

-

8. 1994: Russian hacker stole from Citibank

Lecture Notes

- 1994: Russian hacker stole $10M from Citibank → everything recovered except $400,000

Notes

- *Rober Morris*
- *Vladimir Levin*

9. Y2K+

Lecture Notes

- Y2K+
  - "Denial of Service" in CNN, Yahoo, E-Bay, etc.
  - Attacks on secure sites like FBI, White House, & Microsoft
  - Cyber-terrorism

Notes

- *I Love You virus in the Philippines*

D. Important Hacking Terms & Other interesting terms

1. Back door

Lecture Notes

Notes

- A hole in a security system deliberately left in place by designers intended for use by service technicians

- Maintenance purposes
- Hole in the security systems intended for security services

2. Cracker

Lecture Notes

- One who breaks security on a system
- Coined by hackers in defense against journalistic misuse of the term "hacker"
- The term reflects strong revulsion at the theft & vandalism perpetrated by cracking rings

Notes

-

3. Sneaker

Lecture Notes

- An individual hired to break into places in order to test their security
- Analogous to "tiger team"

Notes

- *Individuals hired to test security*

4. Phreaking

Lecture Notes

- The art & science of cracking a phone network

Notes

- *Cracking a phone*

5. Security through/by obscurity

Lecture Notes

- Hacker term for vendors' favorite way of coping with security holes – namely, ignoring them

Notes

- *Coping bugs, generally ignoring them*

6. Social engineering

Lecture Notes

- A non-technical kind of intrusion that relies heavily on human interaction & often involves tricking other people to break normal security procedures

Notes

- *Deadliest hack get a person easy to manipulate, gather information regarding their security; hypnosis*

7. Deep magic

Lecture Notes

- A security technique central to a program
- In most cases, composed by a "true wizard"
- Many techniques in cryptography, signal processing, graphics, & artificial intelligence are considered deep magic

Notes

- *Security technique normally done by mathematicians to protect accounts in the internet*

8. True Wizard

Lecture Notes

Notes

- A person who knows how a complex piece of software or hardware works
- Someone is a hacker if he/she has general hacking ability, but is a wizard only if he/she has detailed knowledge

- *Casts deep magic, guy who have knowledge of a system or hardware*

9. Virus

Lecture Notes

- A program or piece of code that is loaded onto your computer without your knowledge & runs against your wishes
- Viruses can also replicate themselves

Notes

- *Replicate itself*
- *Infects the **Master Boot Record** via offline mode*

10. Worm

Lecture Notes

- A program or algorithm that replicates itself over computer network & usually performs malicious actions, such as using up the computer's resources & possibly shutting the system down

Notes

- *Replicate using network resources e.g. go through address book, DNS domain network server*

11. Trojan horse

Lecture Notes

- A malicious, security-breaking program disguised as something benign, such as a directory lister, archiver, or game

Notes

- *Malware disguises itself as a benign, utility, time-trigger*

12. Sniffer

Lecture Notes

- Program/device that monitors data travelling over a network
- Can be used both for legitimate network management functions & for stealing information off a network (e.g. password sniffer)
- Can be extremely dangerous since they are virtually impossible to detec and can be inserted almost anywhere

Notes

- *Software useful for hackers, not meant for hacking*
- *Control data over network*
- *Used by hackers*
- *Virtually impossible to detect*

13. Logic bomb / SLAG CODE

Lecture Notes

- Also called "slag code"
- Programming code added to an application / operating system that lies dormant until a predetermined period of time
- Typically malicious in intent, acting in the same

Notes

- *Behaves like a Trojan triggered by event or time*
- *Piece of code BUT built into a legitimate software*

ways as virus or Trojan horse once activated

14. RTFM – "Read the F***ng Manual"

Lecture Notes

- Used by gurus to brush off questions they consider trivial or annoying

Notes

- *Read the fucking manual*

15. Lots of MIPS but no I/O

Lecture Notes

- Person who is technically brilliant but who can't seem to communicate with human beings effectively

Notes

- *SHELDON COOPER, socially inept but brilliant*

16. KISS – Keep It Simple Stupid

17. Foo – term of disgust

E. Standard Hacking Procedure

1. Discovery

Lecture Notes

- "casing" the establishment
- **Footprinting** – process of accumulating data on a network environment to find ways to intrude (looks for vulnerabilities); usually non-intrusive (e.g. company website)
- **Scanning** – searches Internet addresses for any computer particularly vulnerable to a backdoor break-in
- **Enumerating** – listing of information (i.e. users) in a network
- **Sniffing**

Notes

- *FOOTPRINTING – process of accumulating data on network environment to find ways to intrude*
- *E.g. email address, login credentials*
- *SCANNING – computers that are vulnerable, those with no firewall enabled, no anti-virus, or off or outdated, no OS updates especially security updates*
- *ENUMERATING – list of information e.g. email addresses*

2. Penetration & Exploitation

Lecture Notes

- May or may not be malicious

Notes

- *May or may not be malicious*
- *Gained access into the system, penetrate but not exploit*

3. Covering one's tracks

Lecture Notes

Notes

- Disabling auditing
- Clearing event log
- Hiding files

- *Clean up the tracks of your hacking*

F. Types of Hacks

1. System hacking

Lecture Notes

- Breaking into & exposing vulnerabilities of a specific operating system

Notes

- *Hardware or software, we need to hack because is not essentially illegal,*
- *hacked into our system e.g. forgot password, protect with NTFS*
- *Hack into our own accounts, profile*

2. Network hacking

Lecture Notes

- Gaining entry into a specific network

Notes

- *Home networks*
- *WEP not recommended, WPA is*

3. Software/Application hacking

Lecture Notes

- Bypassing software security (e.g. password protection, serial numbers, etc.)

Notes

- *Crack*
- *Serial number & validate in their websites*
- *Easiest among the three*

G. Most Common Attacks

1. Denial of Service (DoS)

Lecture Notes

- Also known as "distributed denial of service"
- With a scanner, hacker looks for vulnerable computers to serve as launch point
- Master computer signals, slave computers simultaneously send out request for information (called "IP packets") that bombard victim's network & shuts it down
- Smurf attack –hacker forges victims address, sends out "ping" to a large network; victim receives overwhelming response

Notes

- *Overwhelm the server*
- *SMURF ATTACK*

2. Buffer overflow

Lecture Notes

- Receiving computer in a network must allocate enough memory for incoming packet
- Programs are vulnerable if size of packet is not checked
- Corruption occurs if data in one buffer overflows into another

Notes

- *Sends the information of how many packets, but more are actually sent than requested*
- *Unaccounted packet go to other parts of main memory & corrupts files → overflow the other segments*

3. Virus, worms & Trojans

4. Footprinting, scanning, enumerating, sniffing

5. Spoofing

Lecture Notes

- Fooling software or hardware
- E-mail spoofing
- IP spoofing

Notes

- *Phishing*
- *Naghahanap ng data gamit yung spoof*
- *Target to get sensitive information*
- *IP Spoofing*
- *DNS Spoofing*
- *DNS (domain name server)*
- *Faster mapping IP addresses and URLs, caches often used sites*
- *ISP level, provides DNS*
- ***CACHE POISONING**: IP address is mapped into the hacker's server; one way of DNS Spoofing*

6. Pilfering

Lecture Notes

-

Notes

- *Copy copyrighted picture*

7. Pornographic pictures & materials

8. Reverse engineering (software hack)

H. Countermeasures

Lecture Notes

- Myth: breaking into a system to test & expose its vulnerability (commonly called “penetration

Notes

- *No secured system*

testing") will minimize if not totally eliminate the hole

- Fact: There a million ways to break into a system!

1. Areas Requiring Protection

a. Physical

Lecture Notes

- Servers, data centers, data storage device

Notes

-

b. Network

Lecture Notes

- Firewall
- Intrusion detection
- Payload security (e.g. encryption)

Notes

- *Encryption payload*

c. Operating System

Lecture Notes

- Built-in security functions (e.g. file permissions, personal firewall, etc.)

Notes

-

d. Application

Lecture Notes

- Authentication using biometrics

Notes

-

2. Prominent Information System Agencies

a. DoD (U.S. Department of Defense)

Lecture Notes

- Established the "Orange Book"
  - Department of Defense Trusted Computer System Evaluation Criteria
  - Provides guidelines in information security implmenetation

Notes

- *ORANGE BOOK: foundation for IT security*
- *Orange kasi yung cover*
- *Neon orange, easy to spot*
- *Example: Do not use a true answer to the security question; no association to you*

b. NCSC (National Computer Security Center)

Lecture Notes

- Established 1983
- Published the Rainbow Series
- Named after the different colors of their covers
- Green Book: Password Management
- Tan Book: A Guide to Understanding Audit in Trusted Systems

Notes

- *RAINBOW SERIES: expanded the Orange Book, with varying colors*
- *EU have newer ones for current standards in IT security*

- Teal Green Book: A Glossary of Computer Security Terms
- Salmon Book: A Guide to Writing the Security Features User's Guide for Trusted Systems

3. Encryption

Lecture Notes

- Process of scrambling data to make it undecipherable to those not authorized to peruse it
- Used to implement "payload security"
- Cryptography – science of encryption & decryption

Notes

- *Make things not understandable to others*
- *USED TO IMPLEMENT PAYLOAD SECURITY: information that travel in the web*
- *CRYPTOGRAPHY: science of encryption & decryption*

a. DES – Data Encryption Standard

Lecture Notes

- Produced by the US National Bureau of Standards
- Approved by ANSI in 1981 for business use
- 20+ years old → aging & getting less secure
- Uses a 56-bit key to encrypt & decrypt a message
- Free for use (no royalties)

Notes

- *Possible values: 2^{56}*
- *Width: 56 bits*
- *Symmetric key cipher*
  - *Only used one key to encrypt and decrypt*

b. IDEA – International Data Encryption Algorithm

Lecture Notes

- Objective is to make DES more secure
- Originally called PES (Proposed Encryption Standard), added 'I' for improved (IPES) → IDEA (International Data Encryption Algorithm)
- Royalties paid to a Swiss company → not widely-used
- Used in PGP ("Pretty Good Privacy", a free encryption software & de facto standard)
- Uses 128-bit encryption
- Only one way to hack: brute force!

Notes

- *With royalties*
- *Width: 128 bits*
- *Possible values: 2^{128}*
- *Also called Triple DES, TDE*
  - *3DES*
  - *TDEA: triple data encryption algorithm*
  - *IDEA*
- *IMPORTANT: KEY & ALGORITHM*

c. Public Key Cryptography

Lecture Notes

- Proposed by Whitfield Diffie & Martin Hellman at Standard University
- Translated into a practical method a year later by Ron Rivest, Adi Shamir, & Leonard Adleman, at the Massachusetts Institute of Technology
- Also known as RSA
- Used as wrapper to transmit a security key (e.g.

Notes

- *Possible Values: 2^{2048}*
- *Width: 2048 bits*
- *Asymmetric Key Cipher: one key to decrypt and another to encrypt*
- *Large pair of keys, and it takes a while to decrypt*

IDEA)

- Generates a pair of keys (very large integers, sometimes 2048 bits or 600+ decimal digits long!) related mathematically in a peculiar but useful way
- Encrypts with one key & decrypts with the other
- Chooses one to be the "public key" given out to anyone

- *Used to encrypt keys or small data*

d. Public Key Encryption

Lecture Notes

- Private key is strongly encrypted (e.g. needs password or other authentication to unlock) & kept in the owner's computer; backup kept in safe place
- Can't hackers reproduce the private key? Yes & No!
- Yes: can be reversed engineered (get the prime factors of the "modulus" then raise it to "exponent")
- No: time element
- Disadvantage: Slow! Hence, used only to encrypt short data (e.g. keys) instead of long messages

Notes

-

Sender's choice to encrypt	
Encrypt Private Key	N/A
Encrypt Public Key	N/A: useless kasi siya lang may access nun
Encrypt Receiver's Private Key	N/A if from Sender
Encrypt Receiver's Public Key	YEHEY!!!!

4. Important Terms

a. Symmetric key ciphers

Lecture Notes

- An encryption system that uses only one key to encode & decode messages

Notes

-

b. Ciphertext

Lecture Notes

- The encrypted message

Notes

-

c. Key

Lecture Notes

- Number used for encryption

Notes

-

d. Passphrase

Lecture Notes

- Or password
- Used to unlock the key & decrypt the ciphertext

Notes

-

e. Trusted System

Lecture Notes

- Employs sufficient hardware & software integrity measures to allow its use for processing a range of sensitive or classified information

Notes

- *Trusted Unix O/S*

5. Authentication

Lecture Notes

- Major objective is proof of identity
- Attempts to identify the legitimate user & determines actions he/she is allowed to perform
- Also attempts to find those posing as others

Notes

-

a. Key Elements

i. Person / Group to be authenticated

ii. Distinguishing characteristics

- You know
    - Password
- You have
    - Cellphone, id, laptop
- Somewhere
    - Weakest among the four, location
- Something you are
    - Fingerprint
    - Physical characteristics

iii. Proprietor for system being used

iv. Authentication mechanism

v. Access control mechanism for limiting the actions of authenticated person or group

b. Biometric Authentication (BEHAVIOURAL & PHYSIOLOGICAL)

Lecture Notes

- Automated method for verifying identity of a person based on physiological or behavioral characteristics
- Provides stronger system
- Implemented through *two-factor-authentication* (combines something one knows with something one has)

Notes

- *Arguably the best authentication*

i. Retinal or iris scan

ii. Fingerprint matching

iii. Face geometry

Lecture Notes	Notes
-	- Steriostopic camera: simulates the human eyes - Not as popular as fingerprint - HIGH END FACE RECOGNITION → see through disguises

iv. Hand geometry

Lecture Notes	Notes
-	- Shape of the hand - PALM PRINT → print of palm - Less accurate - Large readers - Used in factories, car engineers, pagmadumi yung kamay

v. Voice recognition

Lecture Notes	Notes
-	- HW & SW are relatively inexpensive - Problem: accuracy, recorded voice & ambient noise

vi. Signature verification

vii. Keystroke dynamics

c. Digital Signature

Lecture Notes	Notes
- Messages crunched down to fixed numbers of bits (messages digest, usually 128) using a hash function - Encrypted message then encoded using sender's private key - File → crunch → hash → sender's private key encrypt = digital signature - A step further: encrypt the entire message!	-

6. Firewall

Lecture Notes	Notes
- Hardware or software that protects a network from	-

intrusion by outside users
- Often associated with protection from unauthorized users on the Internet
- Does not completely isolate a network from other networks
- Can stem form one of two basic policies:
  - Everything not specifically permitted is denied
  - Everything not specifically denied is permitted
- Seeing the glass half-ful or half-empty

a. Firewall Implementation Techniques

i. Packet filtering

Lecture Notes	***Notes***
- Determines whether an information packet (based on source/destination address, port, etc.) should be permitted to pass through the firewall	-

ii. Network Address Translation (NAT)

Lecture Notes	***Notes***
- A technique that translates universal address into an internal address	-

iii. Proxy Server

Lecture Notes	***Notes***
- Aka application level gateway - Much stricter than packet filtering & designed to regulate access only to specific applications	-

iv. Circuit-level gateway

Lecture Notes	***Notes***
- Proxy server without packet processing & filtering; operates on network layer	-

7. Intrusion Detection

Lecture Notes	***Notes***
- Automate applications or manual policies used to investigate possible break-ins	-

a. Raytheon's BladeRunner

Lecture Notes	***Notes***
- Server-based - Monitors network traffic to prevent transmission of sensitive data	-

b. HP's Praesidium

Lecture Notes	***Notes***
- Detects unauthorized access, root exploits, buffer overflows, and other unusual behavior)	-

c. CERT Intruder Detection Checklist

Lecture Notes	***Notes***
- Suggests examining log ifles, system binaries, etc. to see if the system has been compromised	-

I. IT Security in the 21st Century

1. Increasing reliability of systems

2. Self-healing computers

3. Intelligent system for early intrusion detection

4. Intelligent systems in auditing & fraud detection

5. AI in biometrics

6. Expert systems for diagnosis, prognosis, & disaster planning

7. Smart cards

8. Anti-hacker products

9. Ethical issues in implementing security