Hardware

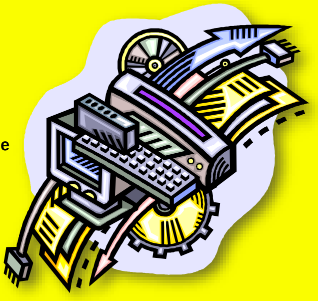
CSH6 Chapter 4

"Hardware Elements of Security"

Sy Bosworth & Stephen Cobb

Topics

- ➢ Introduction
- ➢ Binary Design
- ➢ Parity
- ➢ Hardware Operations
- ➢ Interrupts
- ➢ Memory & Data Storage
- ➢ Time
- ➢ Natural Dangers
- ➢ Data Communications
- ➢ Cryptography
- ➢ Backup
- ➢ Recovery
- ➢ Microcomputers



Introduction

Other hardware-related chapters of CSH6:

- ➢ Ch 5 – Data Communications & Information Security
- ➢ Ch 6 – Network Topologies, Protocols, & Design
- ➢ Ch 22 – Physical Threats to the Information Infrastructure
- ➢ Ch 23 – Protecting the Information Infrastructure

Binary Design

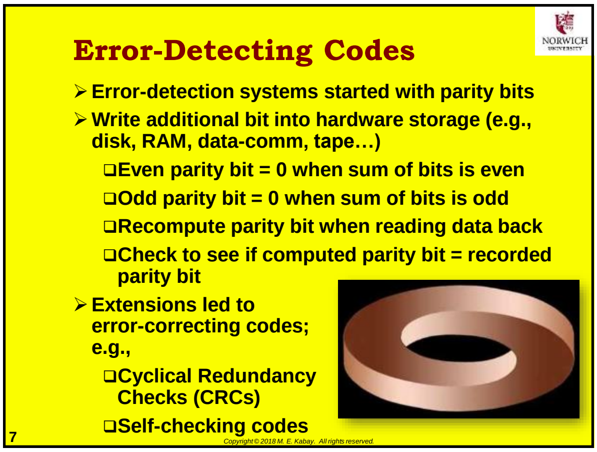
- ➢ Von Neumann Architecture
  - ❑John von Neumann, 1946
  - ❑Apply binary representation to computer implementation
  - ❑Electrical/electronic systems could handle high/low or on/off states to represent binary 0 and binary 1
  - ❑Rapid switching = pulses
- ➢ Pulse characteristics
  - ❑Ideally square waves
  - ❑But cope with sine waves and other waveforms

Circuitry

- ➢ Original 1940s computers used vacuum tubes
  - ❑Relatively large – room-sized machines with power of later calculator-wristwatches
  - ❑Consumed power & ran hot
  - ❑Short MTBF (mean time between failures)
- ➢ Solid-state transistors
  - ❑Patented in 1925 (Lilienfeld) & 1934 (Heil) but never developed
  - ❑William Shockley & colleagues at Bell Labs developed effective transistors starting in 1947

Coding

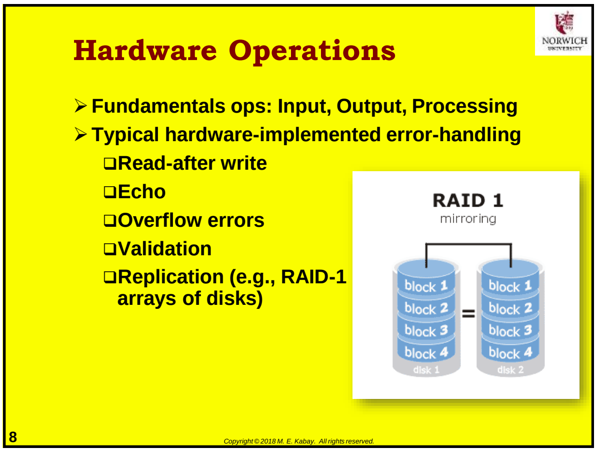
- ➢ Convention for representing data
- ➢ Early codes include
  - ❑Baudot (hence "baud rate")
  - ❑Binary-coded decimal (BCD)
  - ❑Extended BDC (EBCDIC, used by IBM)
  - ❑American Standard Code for Information Interchange (ASCII)
- ➢ Bits → bytes (8 bits/byte) → words (n bytes/word)
- ➢ Prefixes for length of numerical codes (B = bytes & b = bits)
  - ❑KB = kilobyte (1024 bytes) (aka kibibyte!)
  - ❑MB = megabyte (1024 KB) (aka mebibyte)
  - ❑GB = gigabyte (1024 MB) (aka gibibyte)
  - ❑TB = terabyte (1024 GB) (aka tebibyte)



Error-Detecting Codes

- ➢ Error-detection systems started with parity bits
- ➢ Write additional bit into hardware storage (e.g., disk, RAM, data-comm, tape…)
  - ❑ Even parity bit = 0 when sum of bits is even
  - ❑ Odd parity bit = 0 when sum of bits is odd
  - ❑ Recompute parity bit when reading data back
  - ❑ Check to see if computed parity bit = recorded parity bit
- ➢ Extensions led to error-correcting codes; e.g.,
  - ❑ Cyclical Redundancy Checks (CRCs)
  - ❑ Self-checking codes

7

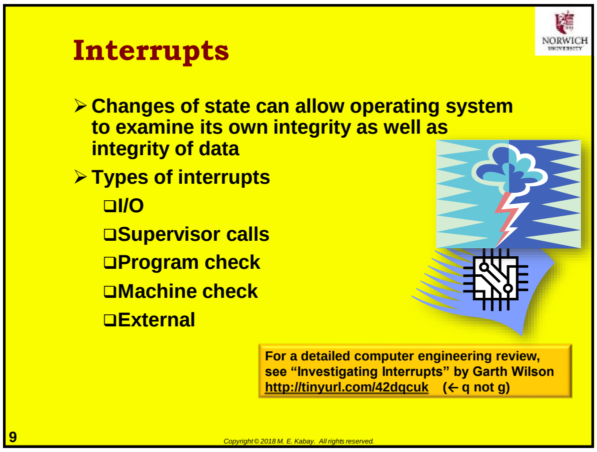


Hardware Operations

- ➢ Fundamentals ops: Input, Output, Processing
- ➢ Typical hardware-implemented error-handling
  - ❑ Read-after write
  - ❑ Echo
  - ❑ Overflow errors
  - ❑ Validation
  - ❑ Replication (e.g., RAID-1 arrays of disks)

RAID 1
mirroring
block 1
block 2
block 3
block 4
disk 1
=
block 1
block 2
block 3
block 4
disk 2

8

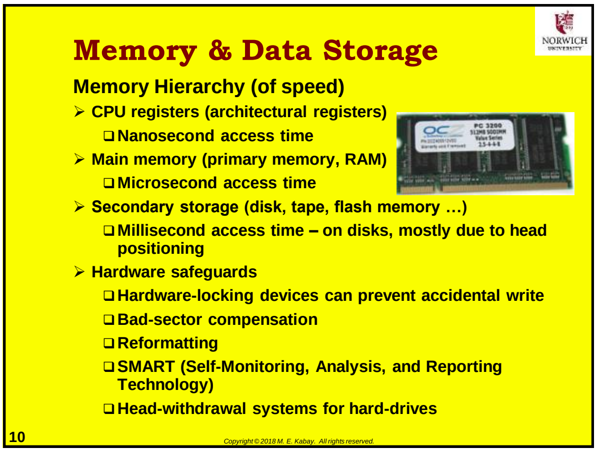


Interrupts

- ➢ Changes of state can allow operating system to examine its own integrity as well as integrity of data
- ➢ Types of interrupts
  - ❑ I/O
  - ❑ Supervisor calls
  - ❑ Program check
  - ❑ Machine check
  - ❑ External

For a detailed computer engineering review, see "Investigating Interrupts" by Garth Wilson http://tinyurl.com/42dqcuk (← q not g)

9

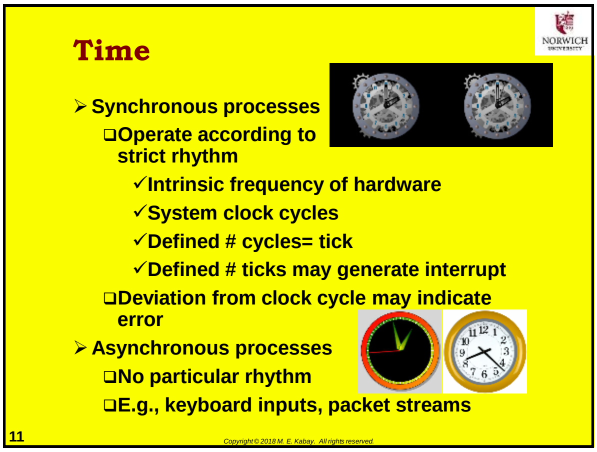


Memory & Data Storage

Memory Hierarchy (of speed)

- ➢ CPU registers (architectural registers)
  - ❑ Nanosecond access time
- ➢ Main memory (primary memory, RAM)
  - ❑ Microsecond access time
- ➢ Secondary storage (disk, tape, flash memory …)
  - ❑ Millisecond access time – on disks, mostly due to head positioning
- ➢ Hardware safeguards
  - ❑ Hardware-locking devices can prevent accidental write
  - ❑ Bad-sector compensation
  - ❑ Reformatting
  - ❑ SMART (Self-Monitoring, Analysis, and Reporting Technology)
  - ❑ Head-withdrawal systems for hard-drives

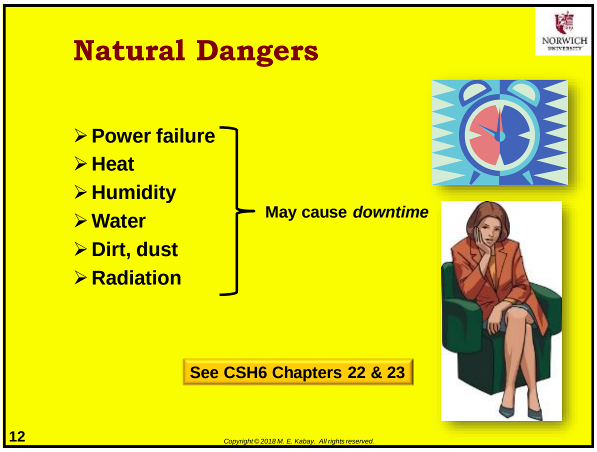
10



Time

- ➢ Synchronous processes
  - ❑ Operate according to strict rhythm
    - ✓ Intrinsic frequency of hardware
    - ✓ System clock cycles
    - ✓ Defined # cycles= tick
    - ✓ Defined # ticks may generate interrupt
  - ❑ Deviation from clock cycle may indicate error
- ➢ Asynchronous processes
  - ❑ No particular rhythm
  - ❑ E.g., keyboard inputs, packet streams

11



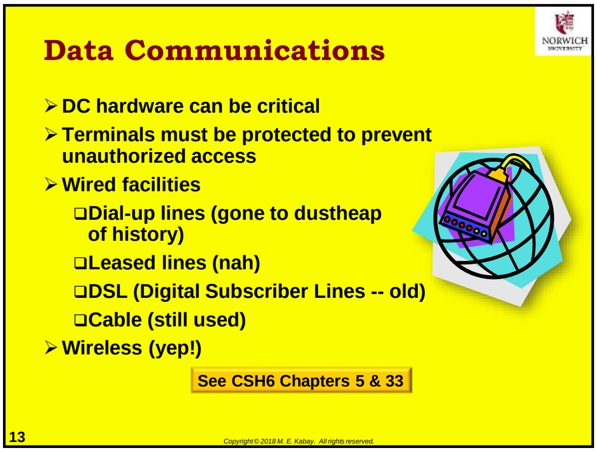
Natural Dangers

- ➢ Power failure
- ➢ Heat
- ➢ Humidity
- ➢ Water
- ➢ Dirt, dust
- ➢ Radiation

May cause *downtime*

See CSH6 Chapters 22 & 23

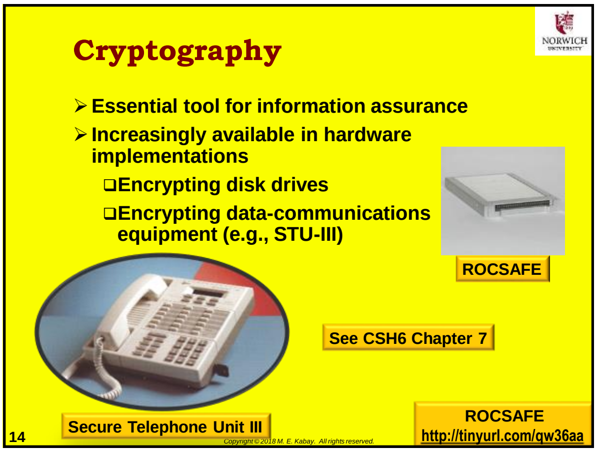
12



Data Communications

- DC hardware can be critical
- Terminals must be protected to prevent unauthorized access
- Wired facilities
  - ❑Dial-up lines (gone to dustheap of history)
  - ❑Leased lines (nah)
  - ❑DSL (Digital Subscriber Lines -- old)
  - ❑Cable (still used)
- Wireless (yep!)

See CSH6 Chapters 5 & 33



Cryptography

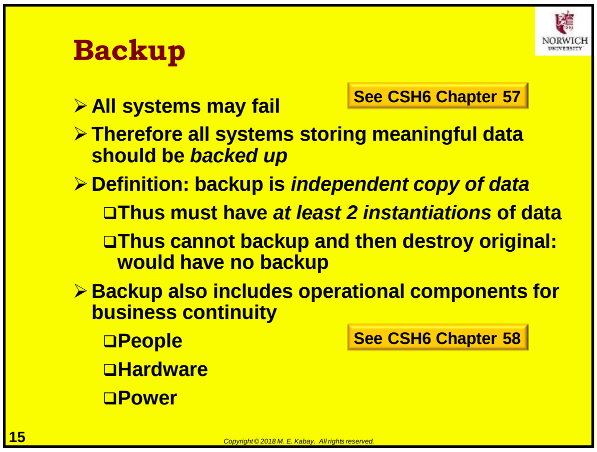
- Essential tool for information assurance
- Increasingly available in hardware implementations
  - ❑Encrypting disk drives
  - ❑Encrypting data-communications equipment (e.g., STU-III)

ROCSAFE

See CSH6 Chapter 7

Secure Telephone Unit III

ROCSAFE
http://tinyurl.com/qw36aa

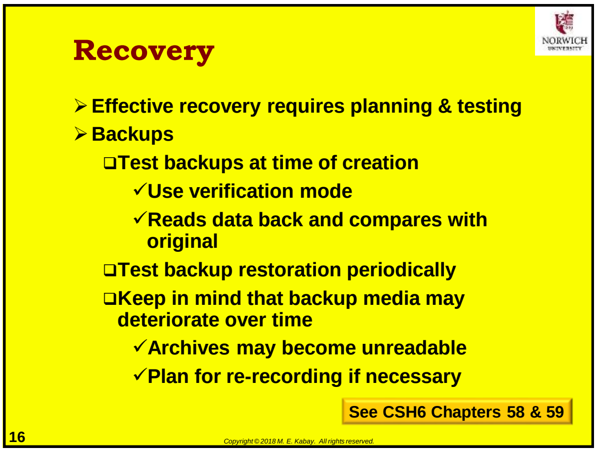


Backup

See CSH6 Chapter 57

- All systems may fail
- Therefore all systems storing meaningful data should be *backed up*
- Definition: backup is *independent copy of data*
  - ❑Thus must have *at least 2 instantiations* of data
  - ❑Thus cannot backup and then destroy original: would have no backup
- Backup also includes operational components for business continuity
  - ❑People
  - ❑Hardware
  - ❑Power

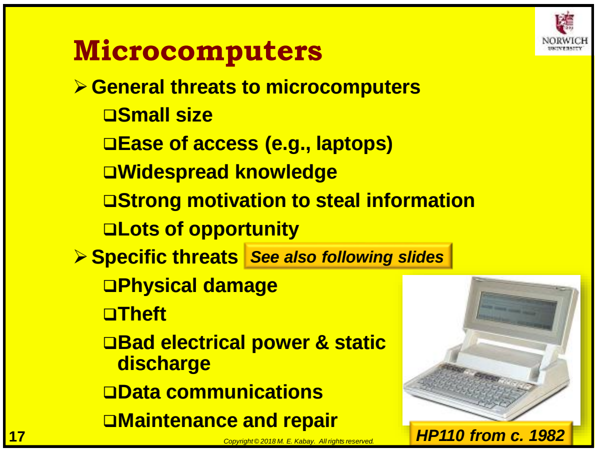
See CSH6 Chapter 58



Recovery

- Effective recovery requires planning & testing
- Backups
  - ❑Test backups at time of creation
    - ✓Use verification mode
    - ✓Reads data back and compares with original
  - ❑Test backup restoration periodically
  - ❑Keep in mind that backup media may deteriorate over time
    - ✓Archives may become unreadable
    - ✓Plan for re-recording if necessary

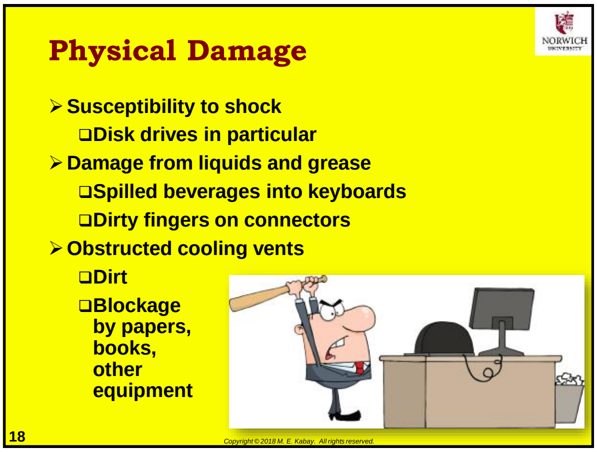
See CSH6 Chapters 58 & 59



Microcomputers

- General threats to microcomputers
  - ❑Small size
  - ❑Ease of access (e.g., laptops)
  - ❑Widespread knowledge
  - ❑Strong motivation to steal information
  - ❑Lots of opportunity
- Specific threats *See also following slides*
  - ❑Physical damage
  - ❑Theft
  - ❑Bad electrical power & static discharge
  - ❑Data communications
  - ❑Maintenance and repair

HP110 from c. 1982

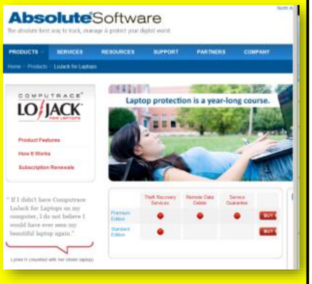


Physical Damage

- Susceptibility to shock
  - ❑Disk drives in particular
- Damage from liquids and grease
  - ❑Spilled beverages into keyboards
  - ❑Dirty fingers on connectors
- Obstructed cooling vents
  - ❑Dirt
  - ❑Blockage by papers, books, other equipment

Theft

- Theft of laptops → loss of control over confidential data
  - ❑Confidential data *must* be encrypted
  - ❑Personally identifiable information (PII) in particular must be encrypted
  - ❑Use whole-disk encryption for simplicity
- Computer lo-jack systems available



AbsoluteSoftware

The absolute best way to track, manage & protect your digital world

PRODUCTS · SERVICES · RESOURCES · SUPPORT · PARTNERS · COMPANY

Home › Products › LoJack for Laptops

COMPUTRACE LO/JACK FOR LAPTOPS

Product Features

How It Works

Subscription Renewals

"If I didn't have Computrace LoJack for Laptops on my computer, I do not believe I would have ever seen my beautiful laptop again."

Laptop protection is a year-long course.

	Theft Recovery Services	Remote Data Delete	Service Guarantee	
Premium Edition	●	●	●	BUY
Standard Edition	●			BUY

http://www.absolute.com/products/lojack

19

Bad Electrical Power & Static Discharge

- Reduce or eliminate use of multiple-access to power outlets
- Add voltage-regulators
  - ❑Prevent spikes and brownouts
  - ❑Many UPSs include voltage regulation
- Don't allow vacuum cleaners (etc) on same circuit as computer systems

See Kabay (2009) "Preparing for the Next Solar Max"
http://www.mekabay.com/infosecmgmt/solarmax.pdf

20

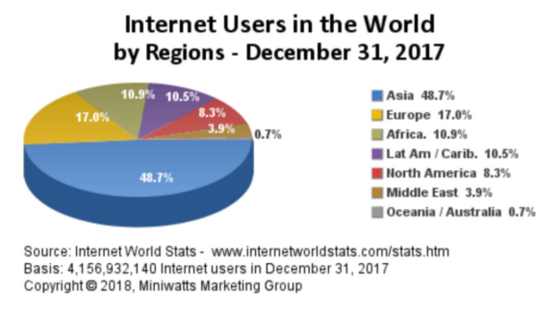
Data Communications

- Explosion of interconnectivity
  - ❑<1980 almost all computer networks were local
    - ✓Simple terminals hardwired to mainframes
    - ✓Smart terminals with some local processing
  - ❑In 1980s LANs interconnected PCs locally
    - ✓WANs and MANs implemented internetworking
    - ✓Internet grew to 1.1M nodes by 1991
  - ❑1990s saw explosion in size of Internet
    - ✓.com TLD (top-level domain) opened ~1993
    - ✓WWW established early 1990s

21

Current Data about Internet (1)

- Regularly updated data @ http://www.internetworldstats.com/stats.htm

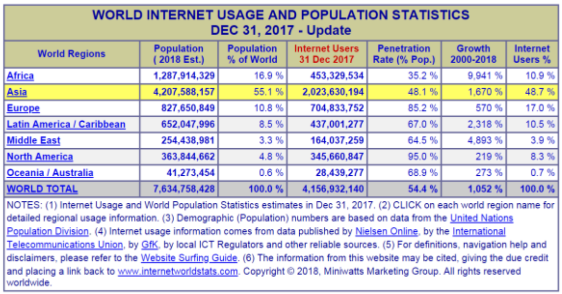


Internet Users in the World by Regions - December 31, 2017

Source: Internet World Stats - www.internetworldstats.com/stats.htm
Basis: 4,156,932,140 Internet users in December 31, 2017
Copyright © 2018, Miniwatts Marketing Group

22

Current Data about Internet (2)



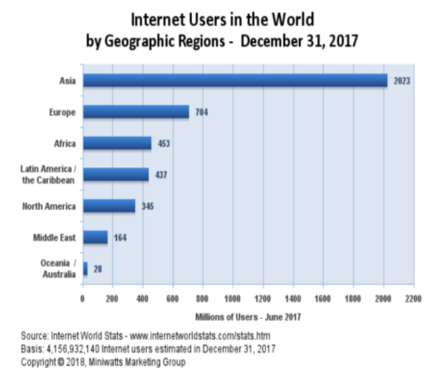
WORLD INTERNET USAGE AND POPULATION STATISTICS
DEC 31, 2017 - Update

World Regions	Population (2018 Est.)	Population % of World	Internet Users 31 Dec 2017	Penetration Rate (% Pop.)	Growth 2000-2018	Internet Users %
Africa	1,287,914,329	16.9 %	453,329,534	35.2 %	9,941 %	10.9 %
Asia	4,207,588,157	55.1 %	2,023,630,194	48.1 %	1,670 %	48.7 %
Europe	827,650,849	10.8 %	704,833,752	85.2 %	570 %	17.0 %
Latin America / Caribbean	652,047,996	8.5 %	437,001,277	67.0 %	2,318 %	10.5 %
Middle East	254,438,981	3.3 %	164,037,259	64.5 %	4,893 %	3.9 %
North America	363,844,662	4.8 %	345,660,847	95.0 %	219 %	8.3 %
Oceania / Australia	41,273,454	0.6 %	28,439,277	68.9 %	273 %	0.7 %
WORLD TOTAL	7,634,758,428	100.0 %	4,156,932,140	54.4 %	1,052 %	100.0 %

NOTES: (1) Internet Usage and World Population Statistics estimates in Dec 31, 2017. (2) CLICK on each world region name for detailed regional usage information. (3) Demographic (Population) numbers are based on data from the United Nations Population Division. (4) Internet usage information comes from data published by Nielsen Online, by the International Telecommunications Union, by GfK, by local ICT Regulators and other reliable sources. (5) For definitions, navigation help and disclaimers, please refer to the Website Surfing Guide. (6) The information from this website may be cited, giving the due credit and placing a link back to www.internetworldstats.com. Copyright © 2018, Miniwatts Marketing Group. All rights reserved worldwide.

23

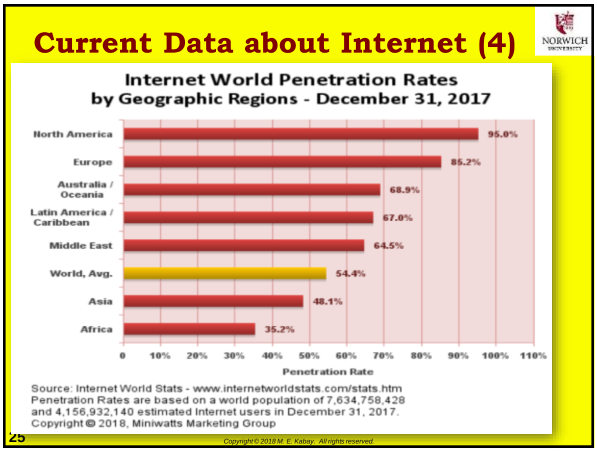
Current Data about Internet (3)



Internet Users in the World
by Geographic Regions - December 31, 2017

Source: Internet World Stats - www.internetworldstats.com/stats.htm
Basis: 4,156,932,140 Internet users estimated in December 31, 2017
Copyright © 2018, Miniwatts Marketing Group

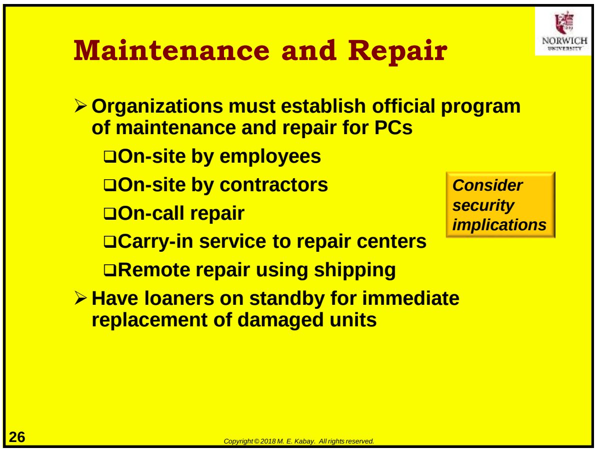
24



Current Data about Internet (4)

Source: Internet World Stats - www.internetworldstats.com/stats.htm
Penetration Rates are based on a world population of 7,634,758,428
and 4,156,932,140 estimated Internet users in December 31, 2017.
Copyright © 2018, Miniwatts Marketing Group

25

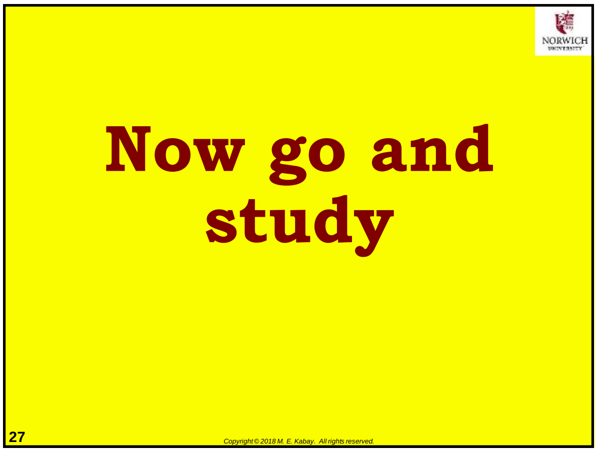


Maintenance and Repair

- Organizations must establish official program of maintenance and repair for PCs
  - ❑On-site by employees
  - ❑On-site by contractors
  - ❑On-call repair
  - ❑Carry-in service to repair centers
  - ❑Remote repair using shipping
- Have loaners on standby for immediate replacement of damaged units

Consider security implications

26



Now go and study

27