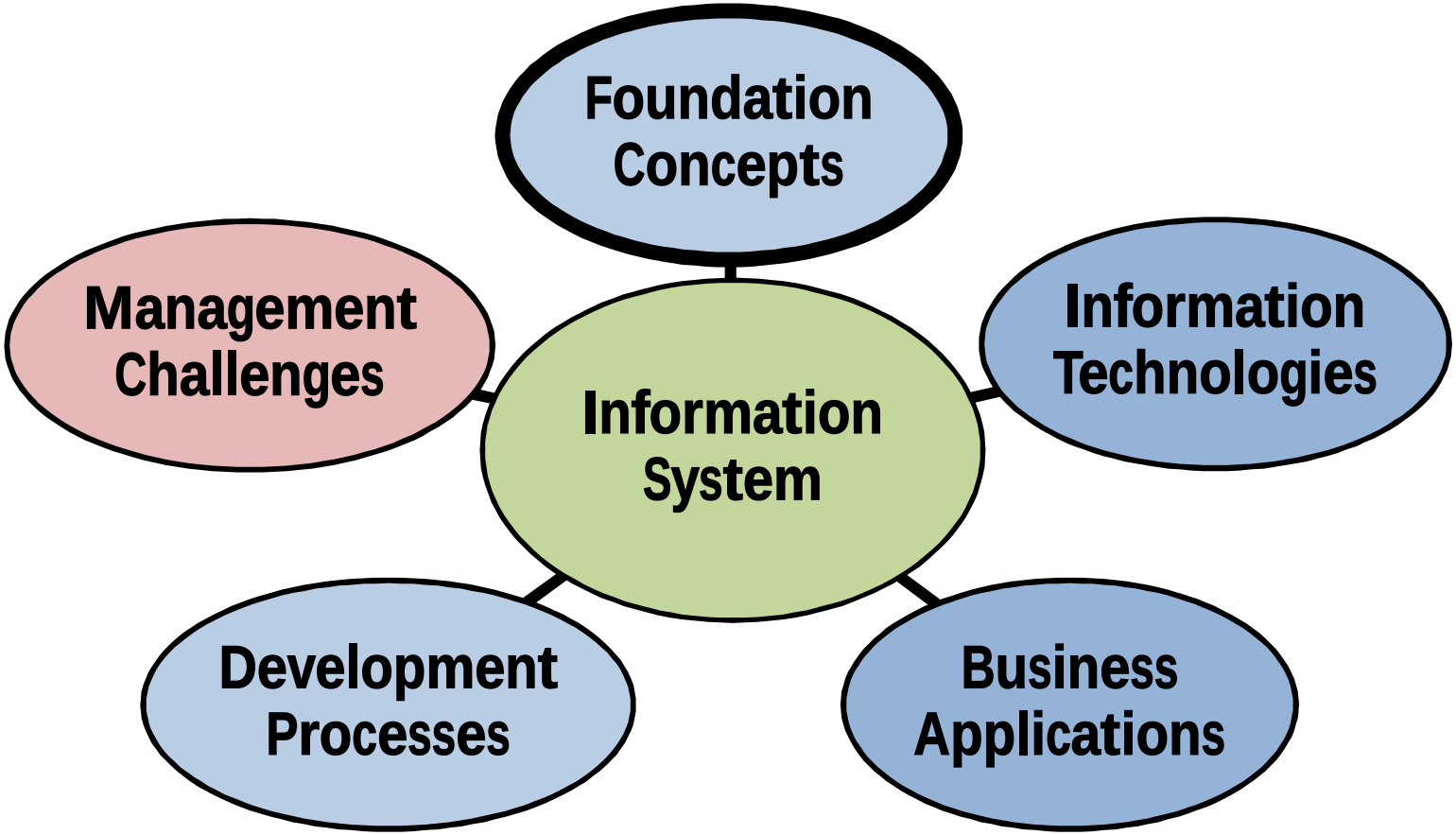
Module V

Management Challenges

The Institute of Management Excellence
E-Mail : info@time.pridepk.com, Web: www.time.pridepk.com

IS Knowledge Framework for Business Professionals

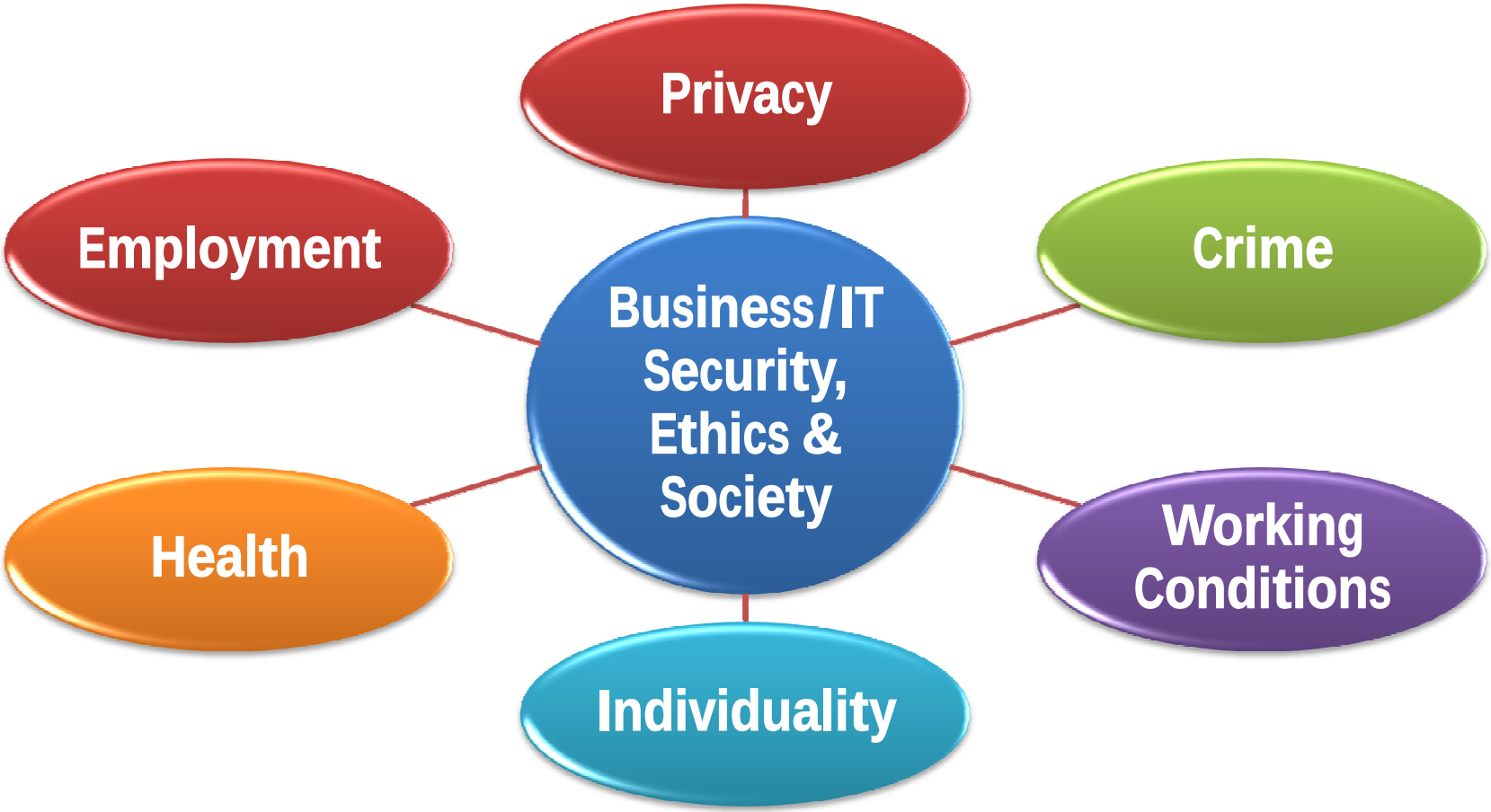


The Institute of Management Excellence
E-Mail : info@time.pridepk.com, Web: www.time.pridepk.com

Security, Ethical & Societal Challenges

The use of IT in business presents **major security challenges**, poses **serious ethical questions** and **affects society** in significant ways.

Security, Ethical & Societal Challenges



Ethical Responsibility

Business professionals have a **responsibility** to **promote ethical uses** of IT in the workplace.

Business Ethics

Questions that managers must confront as **part of their daily business decision making** including:

- Equity
- Rights
- Honesty
- Exercise of Corporate Power

Corporate Social Responsibility Theories

Stockholder Theory

- Managers are agents of the stockholders
- Their only ethical responsibility is to increase the profits of the business
- Without violating the law or engaging in fraudulent practices

Corporate Social Responsibility Theories

Social Contract Theory

- Companies have ethical responsibilities to all members of society
- Which allow corporations to exist based on a social contract

Corporate Social Responsibility Theories

Stakeholder Theory

- Managers have an ethical responsibility to manage a firm for the benefit of all its stakeholders
- Stakeholders are all individuals and groups that have a stake in, or claim on, a company

Principles of Technology Ethics

- Proportionality – the good achieved by the technology must **outweigh** the **harm or risk**. Moreover, there must be no alternative that achieves the same or comparable benefits with less harm or risk
- Informed Consent – those affected by the technology should **understand and accept the risks**

Principles of Technology Ethics

- Justice – the **benefits** and **burdens** of the technology should be **distributed fairly**
- Minimized Risk – even if judged acceptable by the other three guidelines, the technology must be implemented so as to **avoid all unnecessary risk**

Responsible Professional Guidelines

- Acting with integrity
- Increasing your professional competence
- Setting high standards of personal performance
- Accepting responsibility for your work
- Advancing the health, privacy, and general welfare of the public

Computer Crime

- The unauthorized use, access, modification, and destruction of hardware, software, data, or network resources
- The unauthorized release of information
- The unauthorized copying of software
- Denying an end user access to his or her own hardware, software, data, or network resources
- Using or conspiring to use computer or network resources illegally to obtain information or tangible property

Hacking

The **obsessive** use of computers, or the **unauthorized access** and use of networked computer systems

Common Hacking Tactics

Denial of Service

- Hammering a website's equipment with too many requests for information
- Clogging the system, slowing performance or even crashing the site

Scans

- Widespread probes of the Internet to determine types of computers, services, and connections
- Looking for weaknesses

Common Hacking Tactics

Sniffer

- Programs that search individual packets of data as they pass through the Internet
- Capturing passwords or entire contents

Spoofing

- Faking an e-mail address or Web page to trick users into passing along critical information like passwords or credit card numbers

Common Hacking Tactics

Trojan Horse

– A program that, unknown to the user, contains instructions that exploit a known vulnerability in some software

Back Doors

– A hidden point of entry to be used in case the original entry point has been detected or blocked

Common Hacking Tactics

Malicious Applets

– Tiny Java programs that misuse your computer's resources, modify files on the hard disk, send fake e-mail, or steal passwords

War Dialing

– Programs that automatically dial thousands of telephone numbers in search of a way in through a modem connection

Common Hacking Tactics

Logic Bombs

– An instruction in a computer program that triggers a malicious act

Buffer Overflow

– A technique for crashing or gaining control of a computer by sending too much data to the buffer in a computer's memory

Common Hacking Tactics

Password Crackers

- Software that can guess passwords

Social Engineering

- Gaining access to computer systems
- By talking unsuspecting company employees out of valuable information such as passwords

Dumpster Diving

- Sifting through a company's garbage to find information to help break into their computers

Cyber Theft

- Computer crime involving the **theft of money**
- Often inside jobs
- Or use Internet to break in

Unauthorized Use at Work

Time and resource theft

- May range from doing private consulting or personal finances, or playing video games, to unauthorized use of the Internet on company networks

Internet Abuses in the Workplace

- General e-mail abuses
- Unauthorized usage and access
- Copyright infringement/plagiarism
- Newsgroup postings
- Transmission of confidential data
- Pornography – accessing sexually explicit sites
- Hacking
- Non-work related download or upload
- Leisure use of the Internet
- Usage of external ISPs
- Moonlighting

Software Piracy

- Software Piracy
  - Unauthorized copying of computer programs
- **Licensing**
  - Purchase of software is really a payment for a license for fair use
  - Site license allow a certain number of copies
- A third of the software industry's revenues are lost due to piracy

Viruses and Worms

- Virus and worms copy annoying or destructive routines into networked computers
- Often spread via e-mail or file attachments
- Computer Virus
  - Program code that cannot work without being inserted into another program
- Worm
  - Distinct program that can run unaided

Privacy: Opt-in Vs. Opt-out

- Opt-in
  - You explicitly consent to allow data to be compiled about them
  - Law in Europe
- Opt-out
  - Data can be compiled about you unless you specifically request it not be
  - Default in the US

Privacy Issues

- **Violation of Privacy:**
  - Accessing individuals' private e-mail conversations and computer records,
  - Collecting and sharing information about individuals gained from their visits to Internet websites
- **Computer Monitoring:**
  - Always knowing where a person is, especially as mobile and paging services become more closely associated with people rather than places

Privacy Issues

- **Computer Matching**
  - Using customer information gained from many sources to market additional business services
- **Unauthorized Personal Files**
  - Collecting telephone numbers, e-mail addresses, credit card numbers, and other personal information to build individual customer profiles

Protecting your Privacy on the Internet

- E-mail can be encrypted
- Newsgroup postings can be sent through anonymous remailers
- ISP can be asked not to sell your name and personal information to mailing list providers and other marketers
- Decline to reveal personal data and interests on online service and website user profiles

Privacy Laws

Rules that regulate the collection and use of personal data by businesses and the government

Censorship Issues

Spamming

- Indiscriminate sending of unsolicited e-mail messages to many Internet users

Flaming

- Sending extremely critical, derogatory, and often vulgar e-mail messages or newsgroup postings to other users on the Internet or online services

Cyber Law

Laws intended to regulate activities over the Internet or via electronic data communications

Health Issues

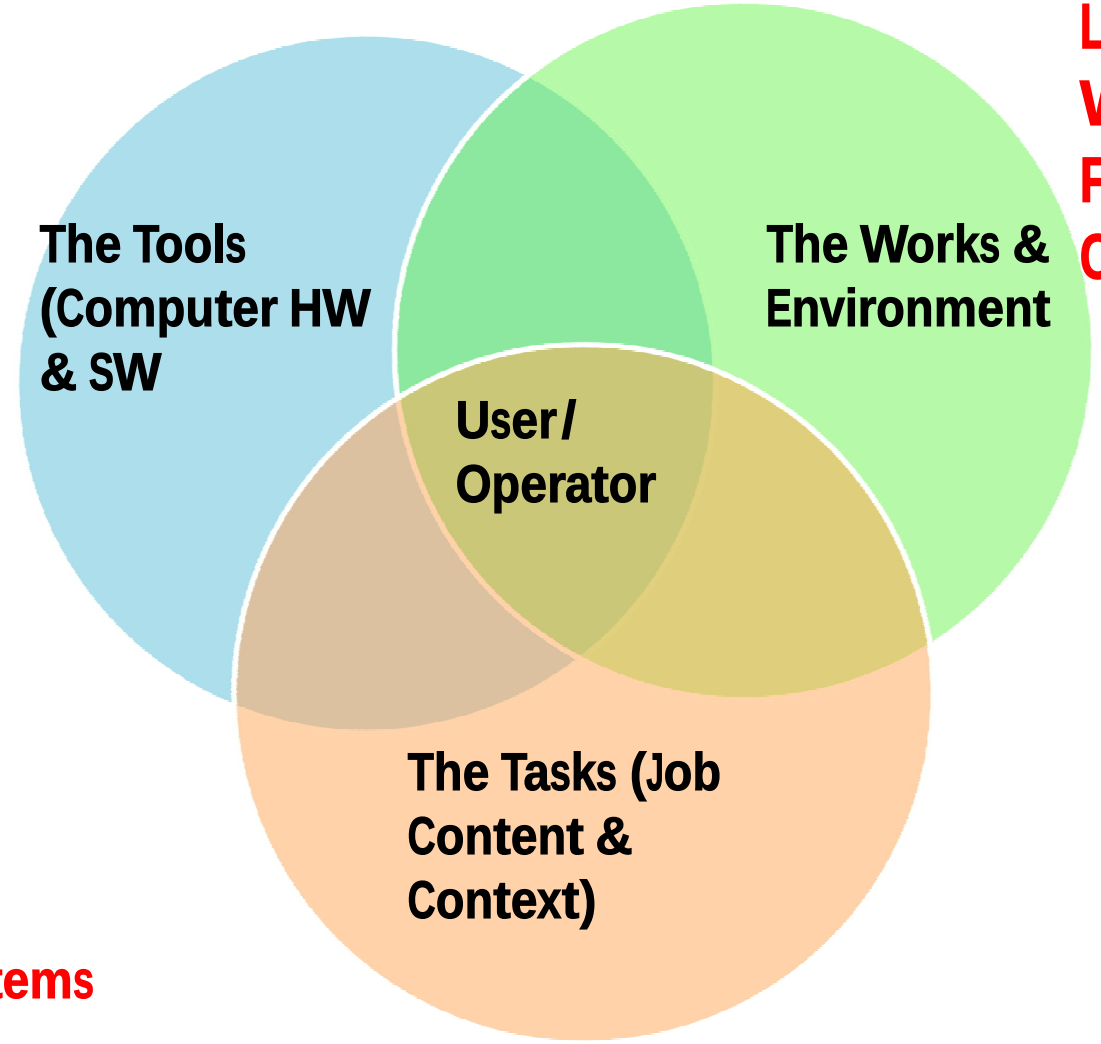
- **Cumulative Trauma Disorders (CTDs)**
  - Disorders suffered by people who sit at a PC or terminal and do fast-paced repetitive keystroke jobs
- **Carpal Tunnel Syndrome**
  - Painful crippling ailment of the hand and wrist

Ergonomics

- Designing **healthy** work environments that are **safe**, **comfortable**, and **pleasant** for **people to work in**
- Thus increasing employee morale and productivity

Ergonomic Factors

Biomechanical
Physical



Lighting
Work Surface
Furniture
Climate

SW Design
Change Training
Job Satisfaction
Support Systems
Shift Work
Management Systems

The Institute of Management Excellence
E-Mail : info@time.pridepk.com, Web: www.time.pridepk.com

Societal Solutions

IT can use to solve human and social problems through societal solutions.

Security Management

- The goal of security management is the **accuracy**, **integrity**, and **safety** of all information system processes and resources.
- Effective security management can **minimize errors**, **fraud** and **losses in the information systems** that interconnect today's companies and their **customers**, **suppliers** and other **stakeholders**

Tools of Security Management

VPN Virtual Private Network	**Firewalls**	**Network Security Protocols**
Encryption	**Security Software Tools**	**Access Control**
Proxy Systems	**Authentication**	**Intrusion Detection**

Internetworked Security Defenses

Encryption

- Data transmitted in scrambled form and unscrambled by computer systems for authorized users only

Internetworked Security Defenses

Firewalls

- A gatekeeper system that protects a company's intranets and other computer networks from intrusion
- By providing a filter and safe transfer point for access to and from the Internet and other networks

- Firewalls are also important for individuals who connect to the Internet with DSL or cable modems

Internetworked Security Defenses

E-mail Monitoring

- Use of content monitoring software that scans for troublesome words that might compromise corporate security

Virus Defenses

- Centralize the distribution and updating of antivirus software
- Use security suite that integrates virus protection with firewalls, Web security, and content blocking features

Computer Failure Controls

- Prevent computer failure or minimize its effects
- Preventative maintenance
- Arrange backups

Fault Tolerant Systems

- Systems that have redundant processors, peripherals, and software that provide a:
  - Fail-over capability to back up components in the event of system failure
  - Fail-safe capability where the computer system continues to operate at the same level even if there is a major hardware or software failure
  - Fail-soft capability where the computer system continues to operate at a reduced but acceptable level in the event of system failure

Disaster Recovery Plan

- Formalized procedures to follow in the event a disaster occurs including:
  - Which employees will participate
  - What their duties will be
  - What hardware, software, and facilities will be used
  - Priority of applications that will be processed
  - Use of alternative facilities
  - Offsite storage of an organization's databases

Information Systems Controls

Methods and devices that attempt to ensure the accuracy, validity, and propriety of information system activities

Auditing IT Security

IT Security Audits

- By internal or external auditors
- Review and evaluate whether proper and adequate security measures and management policies have been developed and implemented

How to Protect Yourself from Cybercrime

1. Use Antivirus and Firewall software and update it often to keep destructive programs off your computer
2. Don’t allow online merchants to store your credit card information for future purchases
3. Use a hard-to-guess password that contains a mix of numbers and letters, and change it frequently

How to Protect Yourself from Cybercrime

4. Use different password for different websites and applications to keep hackers guessing
5. Install all operating system patches and upgrades
6. Use the most up-to-date version of your web browser, email software
7. Send credit card numbers only to secure sites

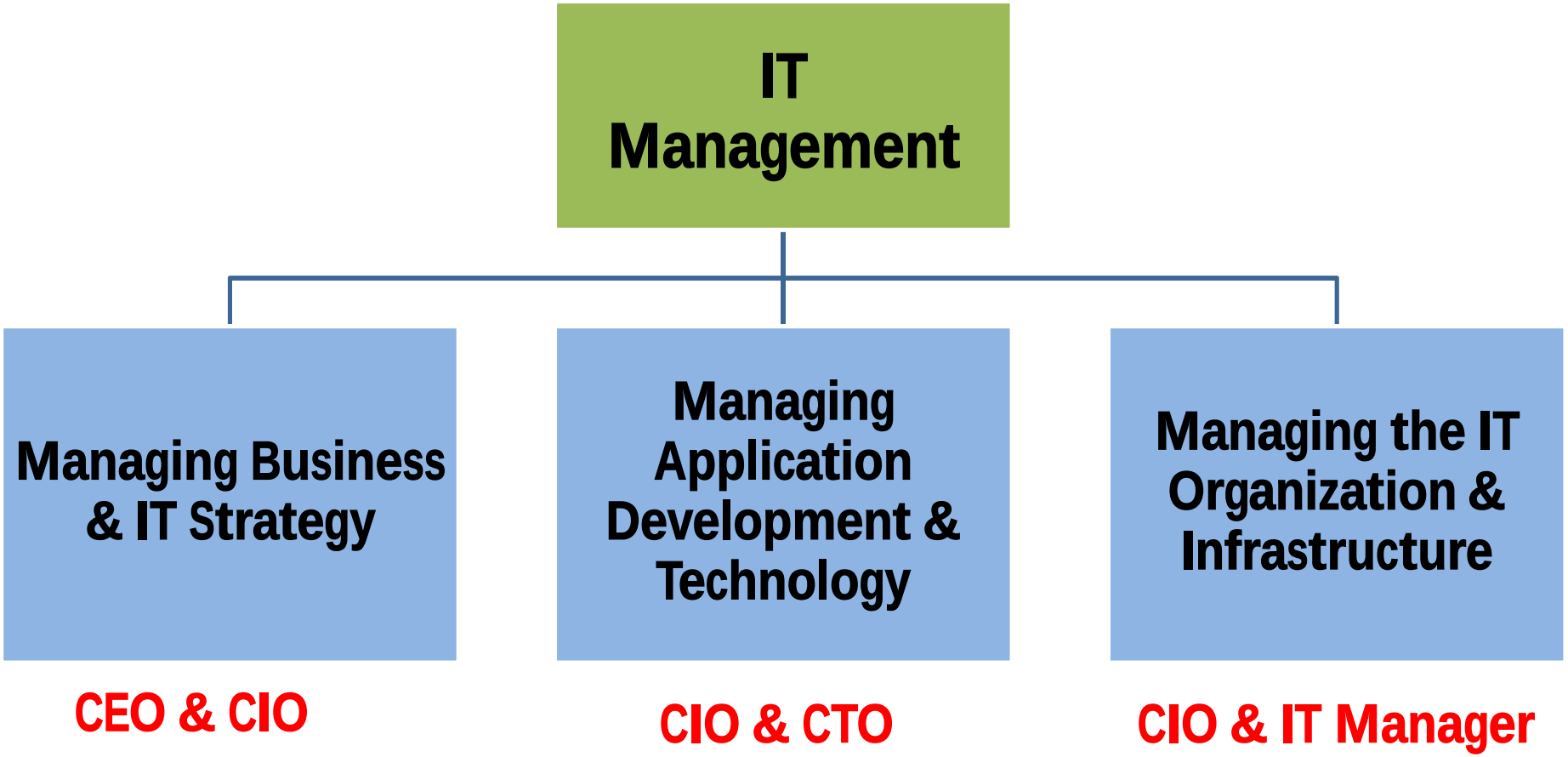
How to Protect Yourself from Cybercrime

8. Use a security program that gives you control over “cookies” that send information back to websites
9. Don’t open email attachments unless you know the source of the incoming message
10. Don’t forget to log off your email account after using

Enterprise and Global Management of IT

- Managing Information Technology
- Managing Global IT

Components of IT Management



Components of IT Management

- Managing the joint development and implementation of business and IT strategies
  - Use IT to support the strategic business priorities
  - Align IT with strategic business goals
- Managing the development and implementation of new business/IT applications and technologies
  - Managing information systems development
- Managing the IT organization and IT infrastructure
  - Hardware, software, database, networks and other resources

Organizing IT

- Early years: centralization of computing with large mainframes
- Next: downsizing trend with a move back to decentralization
- Current: centralized control over the management of IT while serving strategic needs of business units
  - Hybrid of both centralized and decentralized components

Application Development Management

- Managing activities such as:
  - Systems analysis and design, prototyping, applications programming, project management, quality assurance, and system maintenance for all major business/IT development projects

IS Operations Management

- Use of hardware, software, network, and personnel resources in the corporate or business unit data centers of an organization
- Includes computer systems operations, network management, production control and production support
- Data centers are the computer centers of an organization

IT Staff Planning

- Recruiting, training and retaining **qualified IS** personnel
- Evaluate employee job performances and reward outstanding performances with salary increases and promotions
- Set salary and wage levels and design career paths so individuals can move to new jobs through promotion and transfer as they gain in seniority and expertise

Managing User Services

- Business units that support and manage end user and workgroup computing
- Can be done with information centers staffed with user liaison specialists
- Or with Web-enabled intranet help desks

IT Management Failures

IT not used effectively

- Computerize traditional business processes
- Instead of developing innovative e-business processes

IT not used efficiently

- Poor response times and frequent downtimes
- Poorly managed application development projects

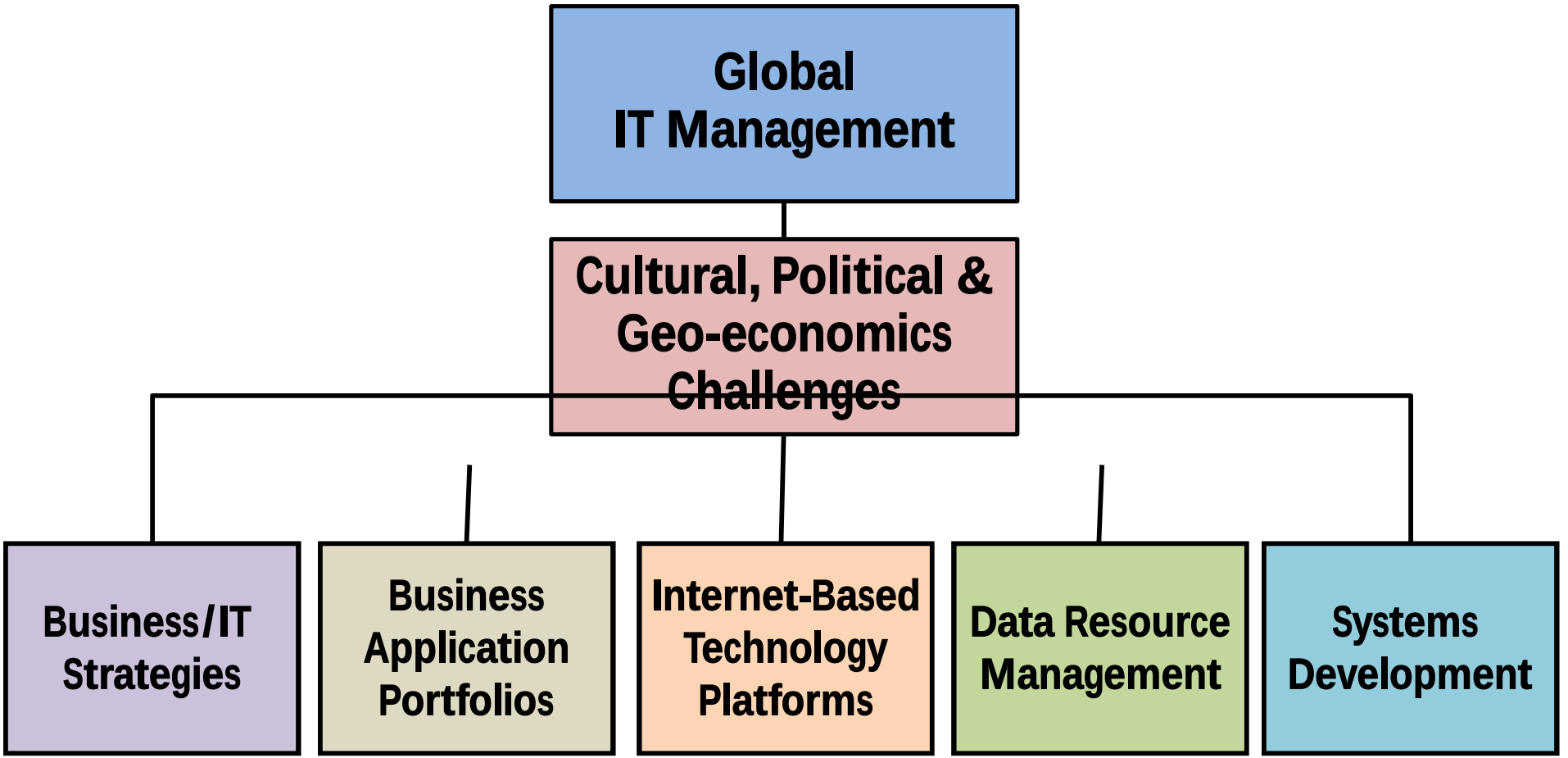
Senior Management's Involvement in BUSINESS/IT Decisions

- How much should we spend on IT?
- Which IT capabilities need to be companywide?
- How good do our IT services really need to be?
- What security and privacy risks will we accept?

Global IT Management

- Develop appropriate business and IT strategies for the **global marketplace**
- Develop the portfolio of business applications needed to support business/IT strategies
- Determine the technology platform needed
- Determine the systems development projects that will produce the required global information systems

Global IT Management Dimensions



Political Challenges

- Rules regulating or prohibiting transfer of data **across national boundaries**
- Severely restricted, taxed, or prohibited imports of hardware and software
- Local content laws that specify the portion of the value of a product that must be added in that country if it is to be sold there
- Reciprocal trade agreements that require a business to spend part of the revenue they earn in a country in that nation's economy

Geoeconomic Challenges

- Sheer physical distances
- Differences in the **cost of living** and **labor costs**
- Difficult to get good-quality telephone and telecommunications services

Cultural Differences

- Languages
- Cultural Interests
- Religions
- Customs
- Social Attitudes
- Political Philosophies

Global Business Drivers

- Business requirements caused by the nature of the industry and its competitive or environmental forces
- Examples of drivers:
  - Global Customers
  - Global Products
  - Global Operations
  - Global Resources
  - Global Collaboration