ĐẠI HỌC TÔN ĐỨC THẮNG
TON DUC THANG UNIVERSITY

Why Study Information Security?

HUYNH NGOC TU, Phd
Faculty of Information Technology

Objectives

- Recognize **the growing importance of information security specialists**
- Develop a **strategy** in the career in **information security**
- Comprehend **information security** in the context of the mission of a **business**

Introduction

- **To protect computers, networks, and the information they store**, organizations are increasingly turning to **information security specialists**
- An information security specialist **is more than a technician who prevents hackers from attacking a Web site**

Introduction

- We begin by trying to answer the first question most students starting out in the field ask: ***Why study information security***?

Growing IT Security Importance and New Career Opportunities

- **Increased services to both end-users and employees create worlds of possibilities in satisfying customer needs, but ...**
- **they also create risks to the confidentiality, integrity, and availability of confidential or sensitive data**

increasing Demand by Government and Private Industry

- **Higher demand for expertly trained individuals**

=> U.S. Statistics

  - The security of computer networks **will continue to increase in importance as more business is conducted over the Internet**

- Computer world expects **security pay to continue to out perform the market**

Becoming an Information Security Specialist

- Get the right certification
  - **Certified Information Systems Security Professional** (CISSP)
  - **Global Information Assurance Certification** (GIAC):www.giac.org
- Consider earning a graduate **degree in INFOSEC**
- Increase your disaster recovery and risk management skills
- Build a home laboratory

Becoming an Information Security Specialist

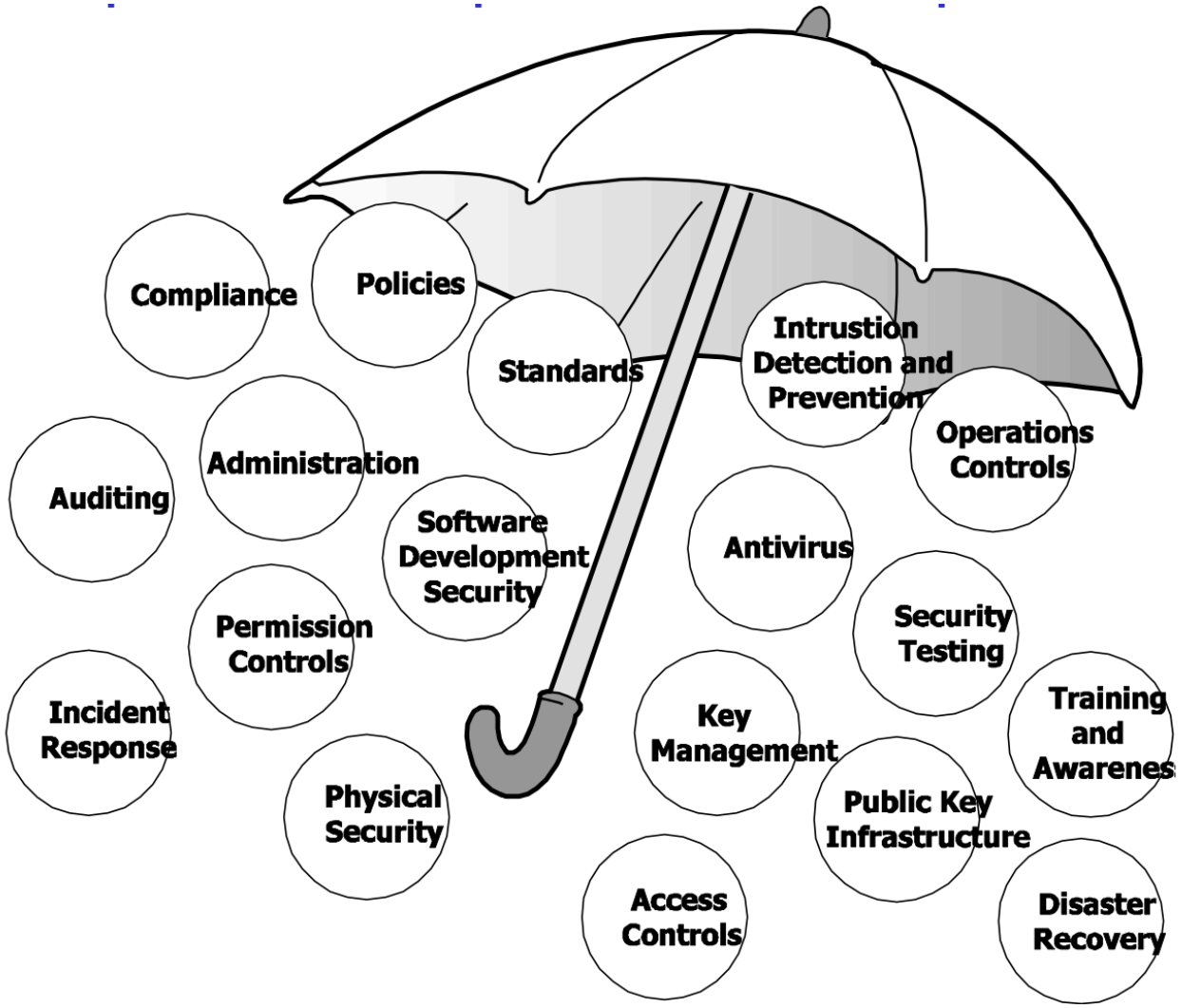
- **Get on a project working with strategic partners**
- Take a second look at government jobs

Schools Are Responding to Demands

- **Hundreds of community colleges, four-year universities, and post-graduate programs are offering degrees** and certificates in emergency preparedness, counterterrorism, and **security**
  - The National Security Agency Centers of Academic Excellence

Contextualizing Information Security

- Information security draws upon the best practices and experiences from multiple domains



Here are some key definitions

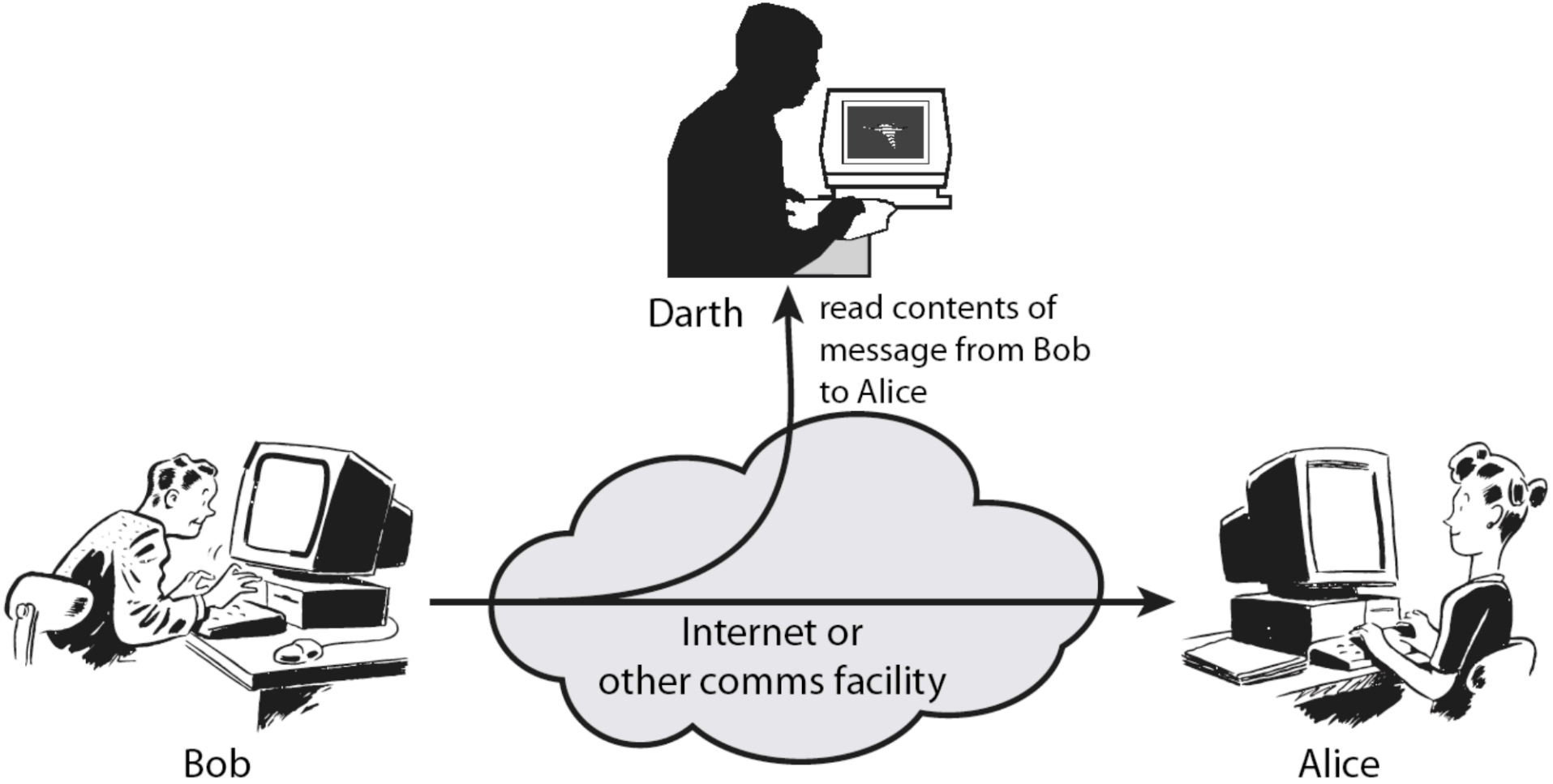
- **Computer Security** - generic name for the collection of tools designed to protect data and to thwart hackers
- **Network Security** - measures to protect data during their transmission
- **Internet Security** - measures to protect data during their transmission over a collection of interconnected networks

Aspects of Security

- consider 3 aspects of information security:
  - **security attack**
  - **security mechanism**
  - **security service**

- The OSI security architecture focuses on security attacks, mechanisms, and services. These can be defined briefly as follows:
- Security attack: Any action that compromises the security of information owned by an organization.
- Security mechanism: A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.
- Security service: A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization.
  - The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

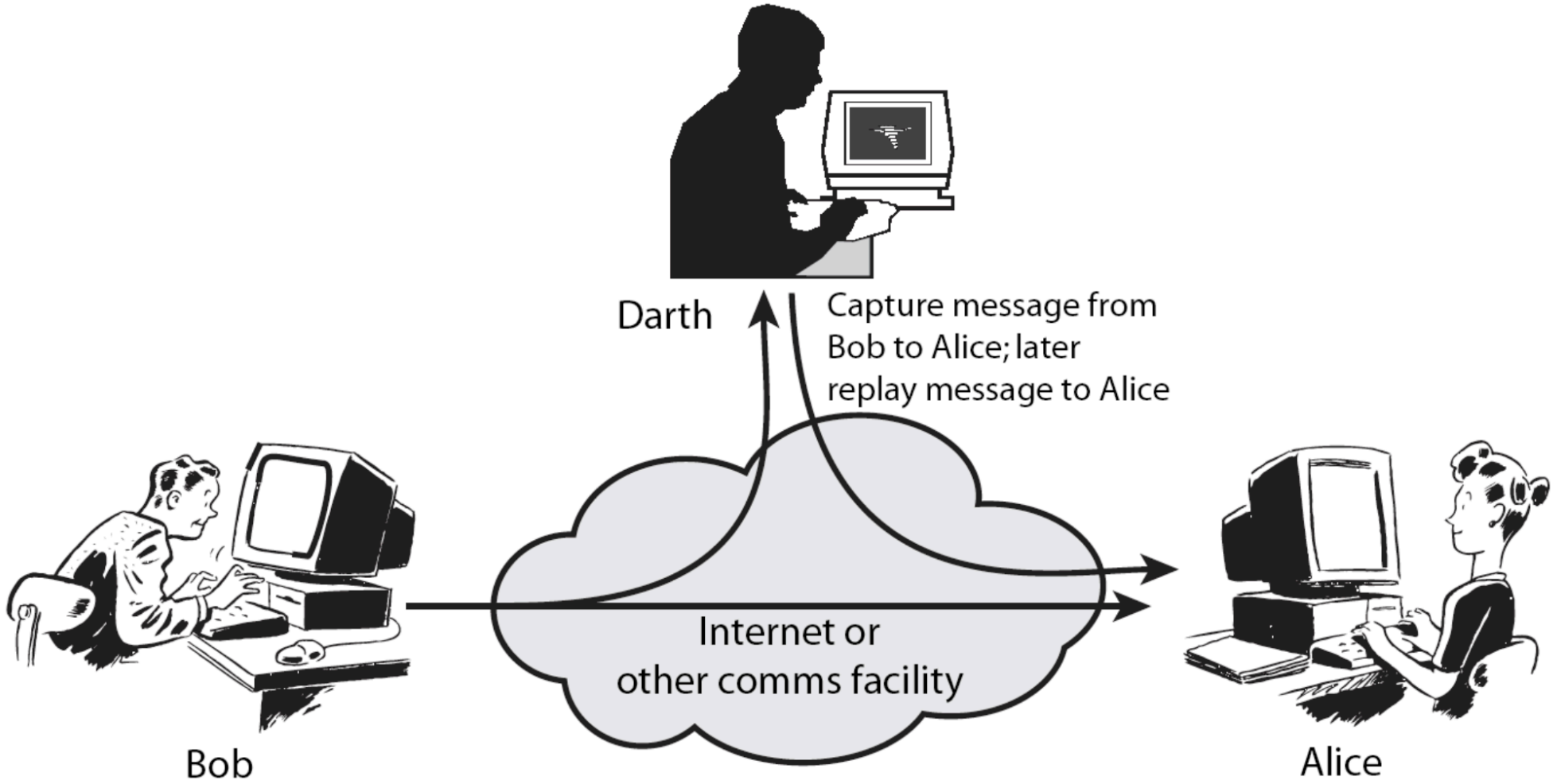
Passive attacks



Passive attacks

- **Have "passive attacks" which** attempt to learn or make use of information from the system but does not affect system resources.
- By eavesdropping on, or monitoring of, transmissions to:
  - obtain message contents (as shown above in Stallings Figure 1.3a), or
  - monitor traffic flows
- **Are difficult to detect** because they do not involve any alteration of the data.

Active attacks



Active attacks

- **Also have "active attacks"** which attempt to alter system resources or affect their operation.
- By modification of data stream to::
  - masquerade of one entity as some other
  - replay previous messages (as shown above in Stallings Figure 1.4b)
  - modify messages in transit
  - denial of service

Security service

- enhance security of data processing systems and information transfers of an organization
- intended to counter security attacks
- using one or more security mechanisms
- often replicates functions normally associated with physical documents
  - which, for example, have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

- *Consider the role of a security service, and what may be required.*
- *Note both similarities and differences with traditional paper documents, which for example:*
  - have signatures & dates;
  - need protection from disclosure, tampering, or destruction;
  - may be notarized or witnessed;
  - may be recorded or licensed

Security service example

- X.800:
  - "a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers"
- RFC 2828:
  - "a processing or communication service provided by a system to give a specific kind of protection to system resources"
- **Note**: security services implement security policies and are implemented by security mechanisms.

Information Security Careers Meet the Needs of Business

- **To support business operations** a number of common positions and career opportunities are needed
- Security administrators
- Access coordinators
- Security architects and network engineers
- Security consultants
- Security testers

Summary

- The risks posed to networked systems **remain to attacks** from **within** and **without** an organization
- The explosive **growth of e-c**ommerce and **business uses of the Internet** have created **a growing demand for INFOSEC specialists**
- The principles, approaches, and concepts in INFOSEC should **work together** to provide the harmonious mix of risk that modern business demands