UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Fakulti Teknologi Maklumat dan Komunikasi

Network Security Administration and Management

BITS 3353

Lecture 1 : Overview of Network Security Administration and Management

Lesson Outline

- Network Administration vs Network Management
- Computer security
- Network security
- Information security
- Security Infrastructure Components
- Goals of security infrastructure
- Design guidelines

security
protection
private
padlock
display
safe
connection
password
technology
detection
electronic
spy
danger
network
concept
sign
firewall
lock
equipment
communication
surveillance
control
video
camera
access
safety
key
web
internet
monitoring
secret
software
safeguard
identity
privacy
data
crime
bodyguard
property
digital
information
close
guard

Security

Security: The state of being free from danger or threat.

Information Security : the state of being protected against the unauthorized use of information, especially electronic data, or the measures taken to achieve this.

Network security: the process of taking physical and software preventive measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby creating a secure platform for computers, users and programs to perform their permitted critical functions within a secure environment.

Security Principles

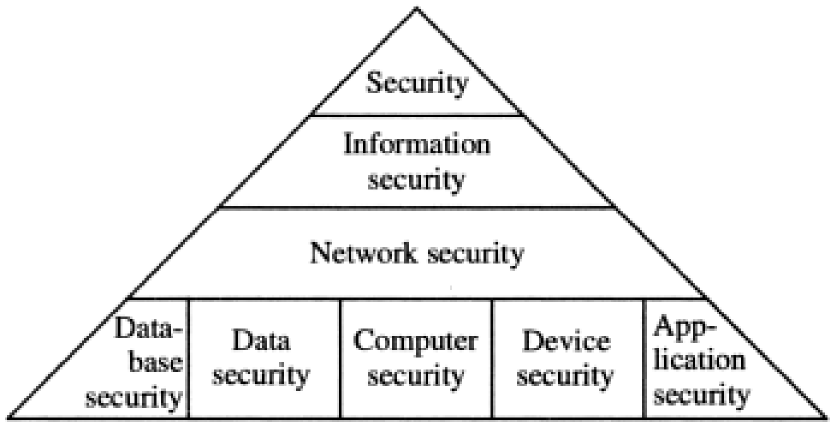


Figure 1.1 The hierarchy of security specializations.

- The field of security is concerned with protecting general assets
- Steps to protect person or property from harm
  - Harm may be intentional or nonintentional
- Sacrifices convenience for safety

Network security administration
vs
network security management

Network security administration

involves configuring hardware, and running cables in a secure manner.

Network security management

involves making decisions about the security of a network

Network managers usually start off as network administrators and may still perform network administration duties, but their technical knowledge guides managerial decisions

4 Components of a Security Infrastructure

Network

Encompasses firewalls, routers, and switches, remote access devices (such as VPNs, and dialup modem banks) and network-based IDS that add some security features to the overall design

These components are used to monitor, filter and/or restrict traffic as seen either by their network interfaces or as defined logic in software

Platforms

Encompasses the server and client side software (such as underlying operating system and security applications controls)

Application-level access controls, such digital certificates, host-based IDS and analysis, virus detection and event accounting and analysis

Physical

Include standard door keys and locks, key cards, identification badges, security cameras, motion sensors, biometric components, cages, fences, guards and systems.

The primary goal of a physical security component is to keep unauthorized persons out and keep infrastructure components supplied with power and network connectivity

Process

Includes corporate security policy and procedural documents that governs the creation, used, storage and disposal of corporate data, as well as the systems and networks on which that data resides

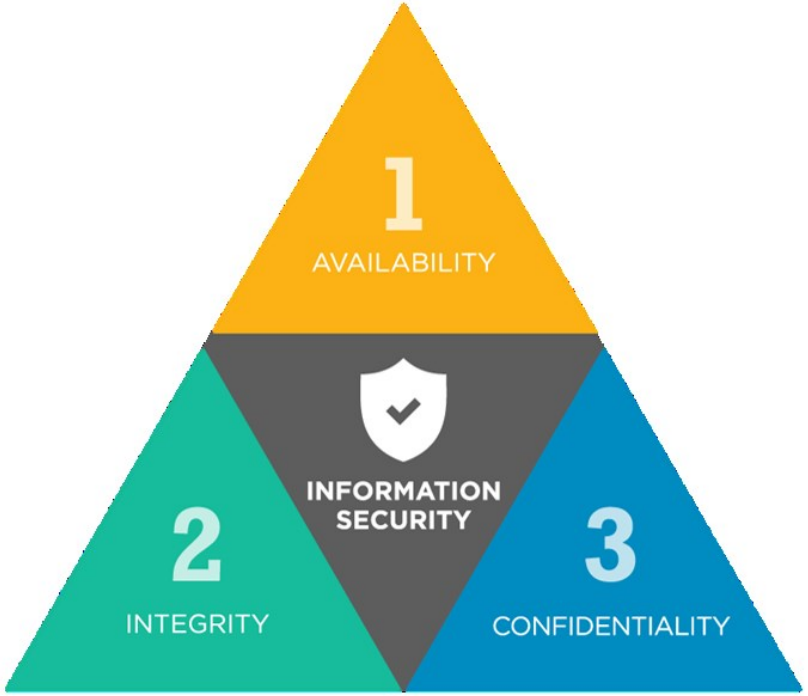
Corporate security procedures, a component of the corporate security policies document, are utilized to guide employee actions in particular circumstances

The purpose of corporate security policy is to define the scope of protection for corporate assets and suggest or require a specific protection mechanism for those assets

Goals of security infrastructure

- The primary goal of a security infrastructure design is the protection of corporate assets
- The controls applied in the protection of these assets should be inline with your corporate security goals as well as your corporate security policy documentation
- Each of the following protection goals should be approximately represented and weighted accordingly:
  - Data confidentiality
  - Data integrity
  - Data availability

CIA Triads



Confidentiality

- Set of rules that limits access to information
- Only authorized users and processes should be able to access or modify data

Integrity

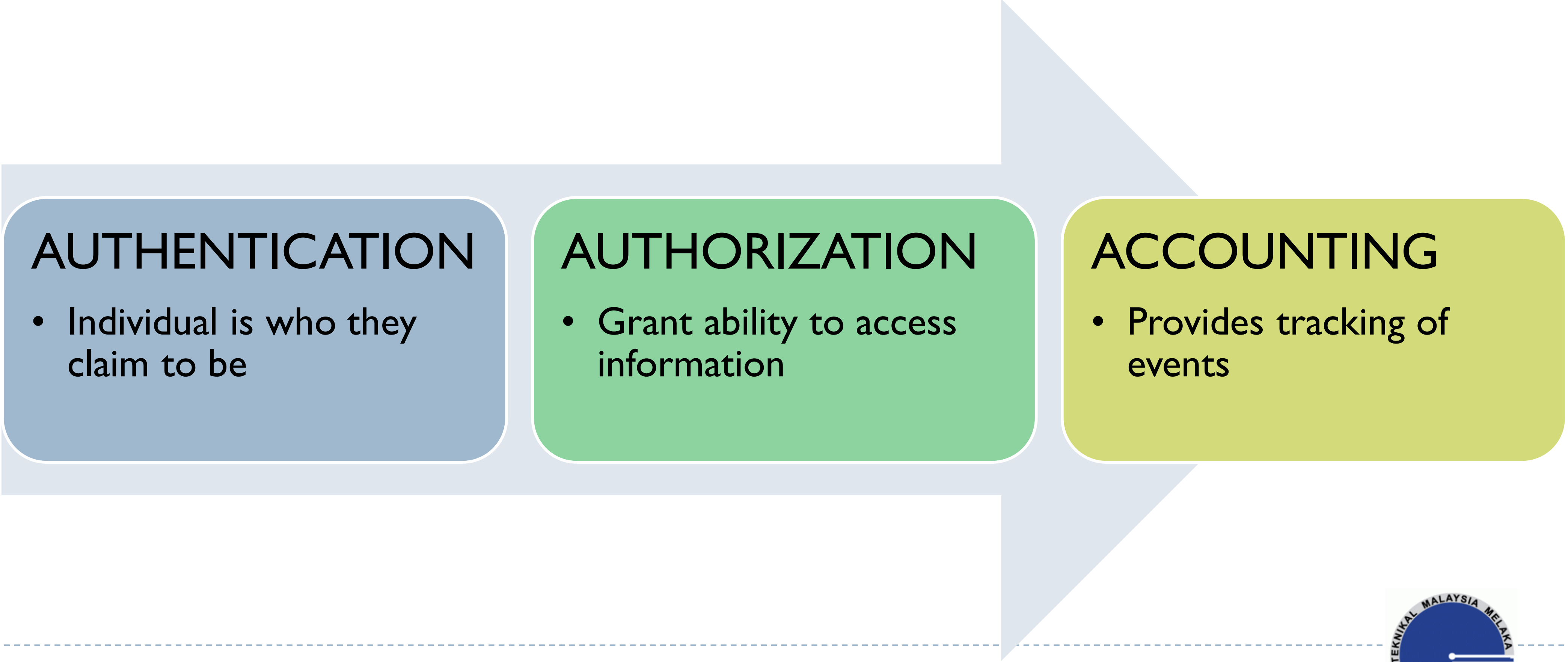
- Assurance that the information is trustworthy and accurate
- Data should be maintained in a correct state and nobody should be able to improperly modify it, either accidentally or maliciously

Availability

- Authorized users should be able to access data whenever they need to do so

Authentication, Authorization and Accounting (AAA) Services

- Protections implemented to secure information



AUTHENTICATION

- Individual is who they claim to be

AUTHORIZATION

- Grant ability to access information

ACCOUNTING

- Provides tracking of events

Vulnerability, Threat and Attack

Vulnerability

- Existence of a flaw or weakness in the system that can lead to an unexpected, undesirable event compromising the security of the system.

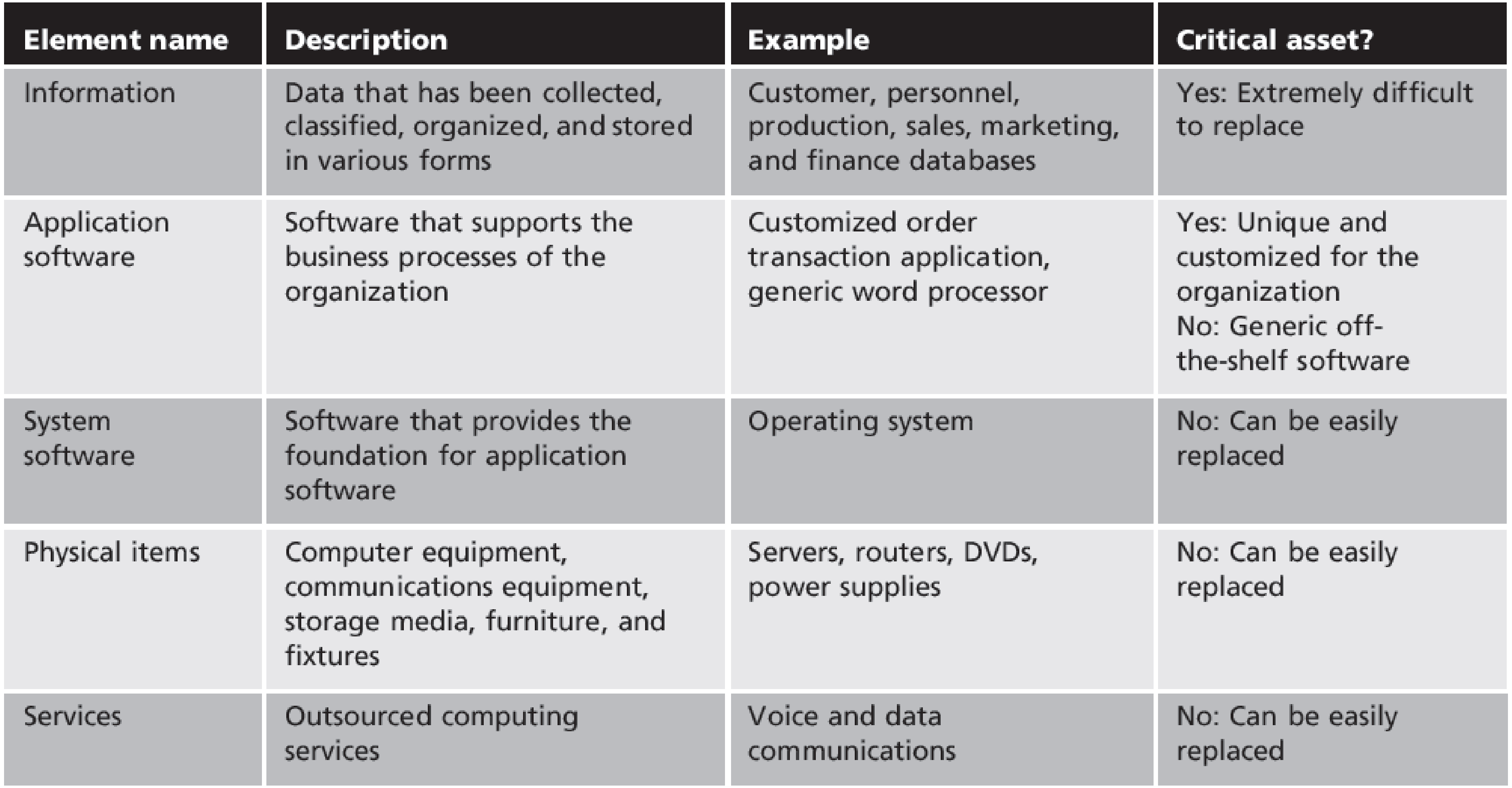
Threat

- An event, person or circumstance that has ability to damage the system by altering, deleting, disclosing or DoS.

Attack

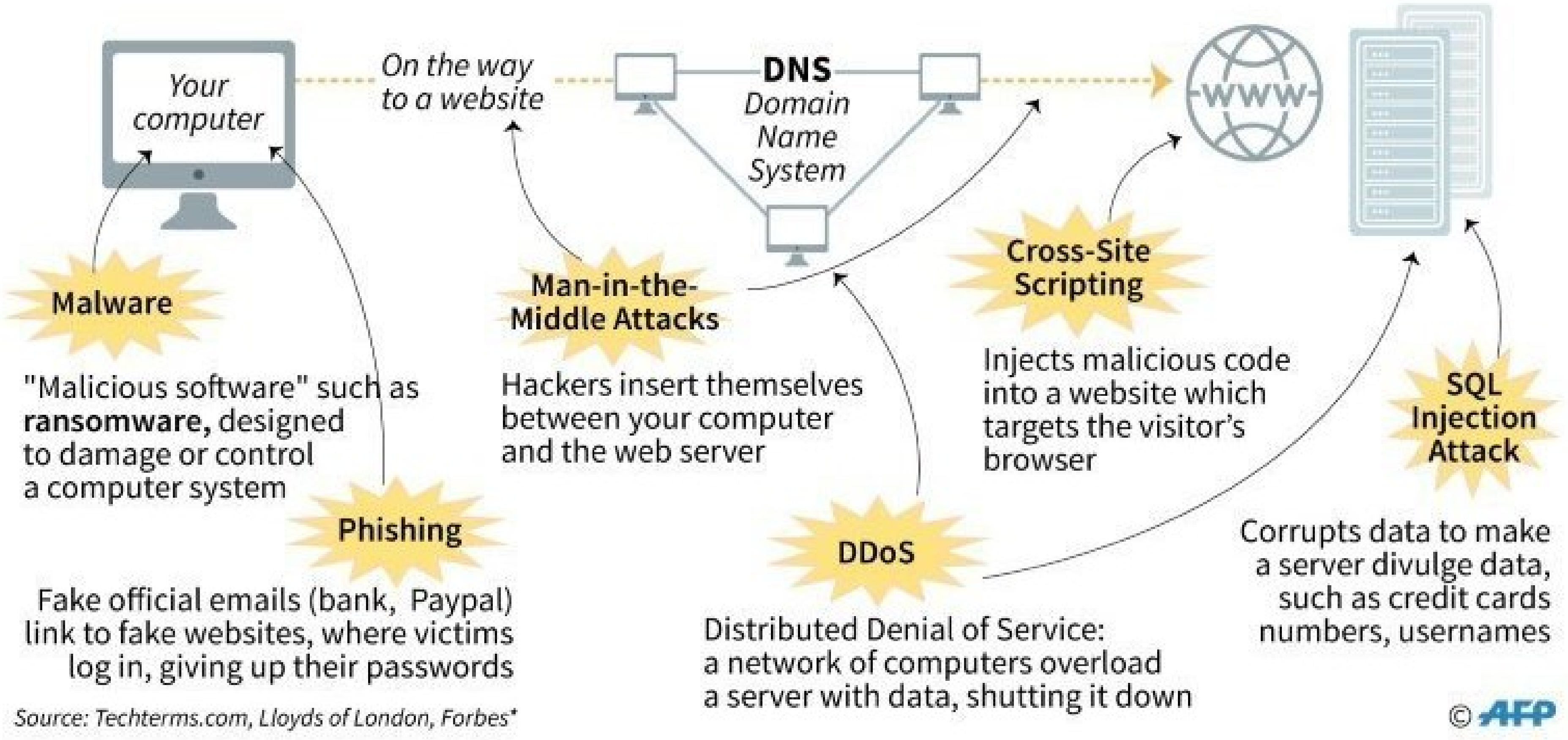
- Is deliberate action of causing harm to the computer systems by exploiting known vulnerabilities and threats.

Information Technology Assets



Element name	Description	Example	Critical asset?
Information	Data that has been collected, classified, organized, and stored in various forms	Customer, personnel, production, sales, marketing, and finance databases	Yes: Extremely difficult to replace
Application software	Software that supports the business processes of the organization	Customized order transaction application, generic word processor	Yes: Unique and customized for the organization No: Generic off-the-shelf software
System software	Software that provides the foundation for application software	Operating system	No: Can be easily replaced
Physical items	Computer equipment, communications equipment, storage media, furniture, and fixtures	Servers, routers, DVDs, power supplies	No: Can be easily replaced
Services	Outsourced computing services	Voice and data communications	No: Can be easily replaced

The different types of cyber attacks



Malware: "Malicious software" such as **ransomware,** designed to damage or control a computer system

Man-in-the-Middle Attacks: Hackers insert themselves between your computer and the web server

Cross-Site Scripting: Injects malicious code into a website which targets the visitor's browser

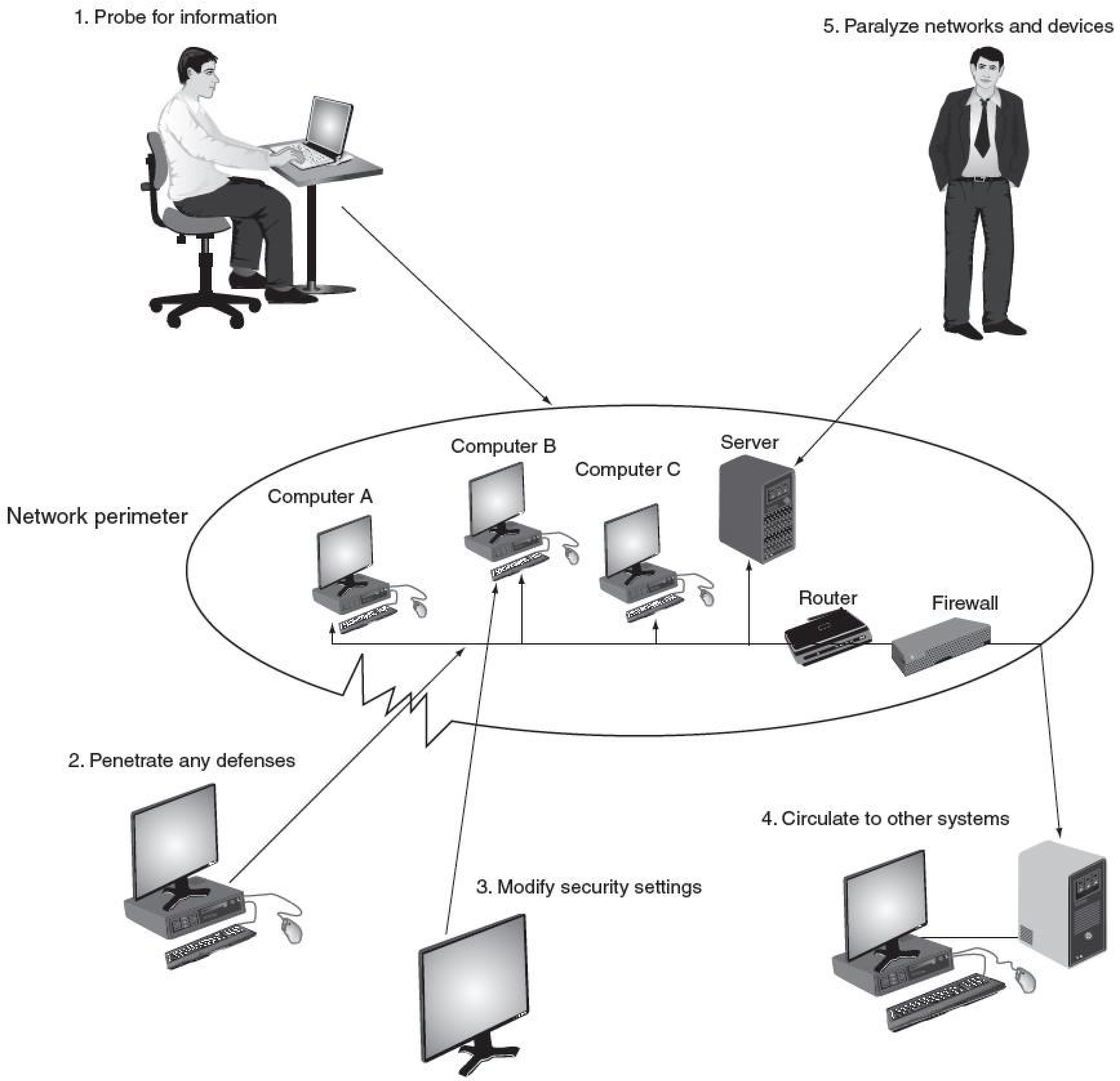
SQL Injection Attack: Corrupts data to make a server divulge data, such as credit cards numbers, usernames

Phishing: Fake official emails (bank, Paypal) link to fake websites, where victims log in, giving up their passwords

DDoS: Distributed Denial of Service: a network of computers overload a server with data, shutting it down

Source: Techterms.com, Lloyds of London, Forbes*

Steps of an Attack


1. Probe for information
5. Paralyze networks and devices
Computer B
Computer C
Server
Computer A
Network perimeter
Router
Firewall
2. Penetrate any defenses
4. Circulate to other systems
3. Modify security settings

Defense Against Attacks

Layering

- Information security must be created in layers
- Layered security approach

Limiting

- Limiting access to information
- Only those who must use data granted access

Diversity

- Closely related to layering
- Layers must be different (diverse)

Obscurity

- Obscuring inside details to outsiders

Simplicity

- Nature of information security is complex
- Complex security systems is difficult to understand and troubleshoot and often compromised for ease of use by trusted users

Summary

Information security attacks growing exponentially in recent years

- Several reasons for difficulty defending against today's attacks
- Information security protects information's integrity, confidentiality, and availability:
    - On devices that store, manipulate, and transmit information
    - Using products, people, and procedures

- Goals of information security
    - Prevent data theft
    - Thwart identity theft
    - Avoid legal consequences of not securing information
    - Maintain productivity
    - Foil cyberterrorism

Thank you