CSC459-ITC459-Security Engineering

System Security

Dr. Mehrdad Sharbaf

CSUDH-CSC

System Security (1 of 4)

Vital part of every computer system

System security concepts

CIA triangle: shows main elements used to develop a security policy

- Confidentiality
- Integrity
- Availability

System Security (2 of 4)

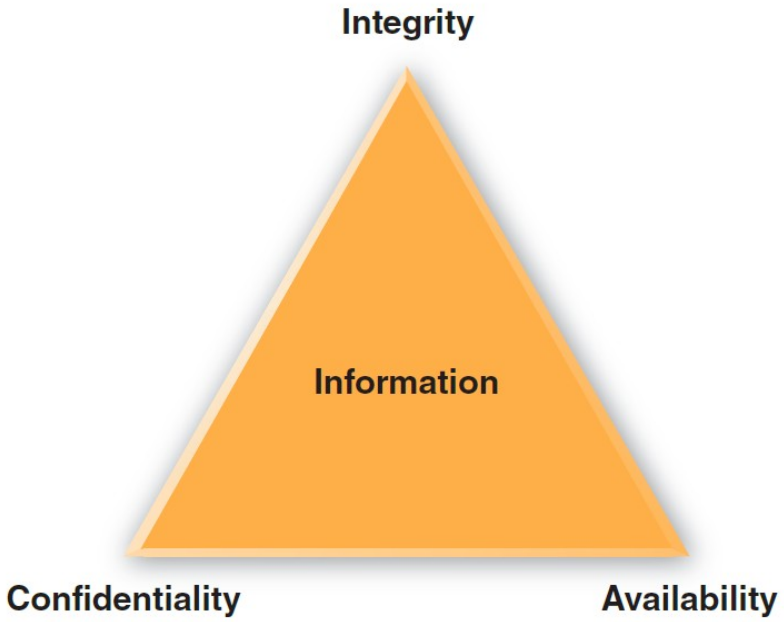


Figure 12-14 System security must provide information confidentiality, integrity, and availability (CIA).

System Security (3 of 4)

- Risk management
  - Risk identification
    - List and classify assets and analyze possible threats
    - Identify vulnerabilities and how they might be exploited
  - Risk assessment
    - Risks need to be calculated and prioritized
  - Risk control
    - Strategies: avoidance, mitigation, transference, and acceptance

System Security (4 of 4)

- **Figure 12-15** Risk management requires continuous risk identification, assessment, and control.

The slides are excerpted from Tilley 12 edition systems analysis and design book

Security Levels (1 of 12)

- System security involves six separated but interrelated levels

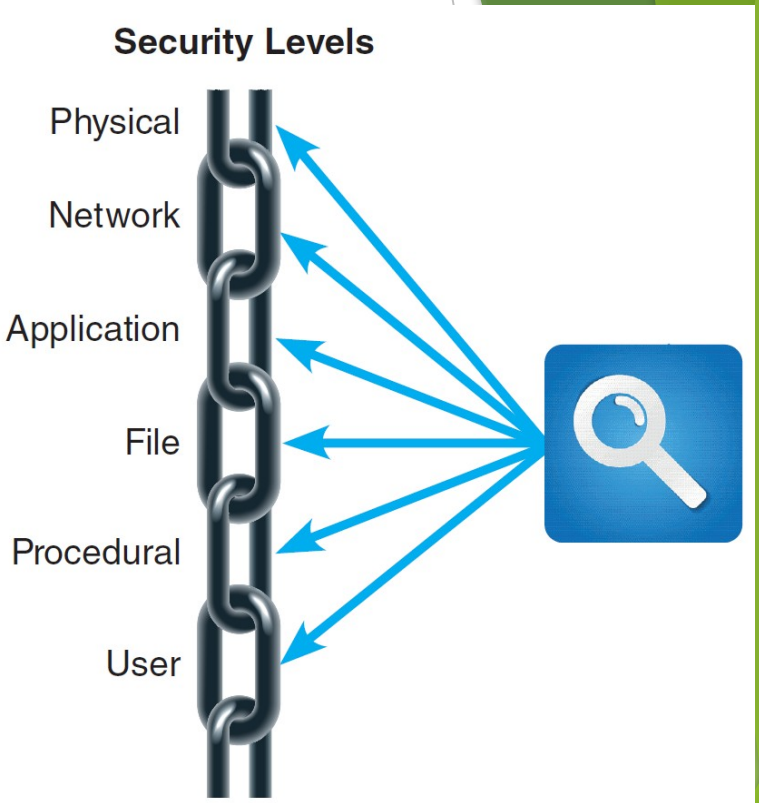


Figure 12-19 Each security link has a specific focus, and the overall chain is only as strong as the weakest link.

The slides are excerpted from Tilley 12 edition systems analysis and design book

Security Levels (2 of 12)

- Physical security
  - Operations center security
    - Each entrance must be equipped with a suitable security device
  - Servers and desktop computers
    - Install locks on server racks to avoid unauthorized placement of keystroke loggers
    - Tamper evident cases and BIOS-level passwords can be used

The slides are excerpted from Tilley 12 edition systems analysis and design book

Security Levels (3 of 12)

- Portable computers
  - Select an operating system with strong protection
  - Mark case with company name and address
  - Consider devices that have a built-in fingerprint reader, facial recognition, and use the Universal Security Slot (USS)
  - Back up all vital data before using the computer outside the office and link the system to a tracking software
  - Use location services
  - Be alert to high-risk situations while traveling
  - Establish stringent password protection policies

Security Levels (4 of 12)

- Network security
  - Encrypt network traffic: private key encryption and public key encryption
  - Wireless networks: WPA2 strengthens the level of wireless protection
  - Private networks can be used when speed is necessary
  - Virtual Private Networks (VPN) establish secure connections for a large number of computers

Security Levels (5 of 12)

Ports and services can be affected by port scans and denial of service (DOS) attacks

- A port routes incoming traffic to the correct application and a service monitors a particular port

Firewalls allow or block network traffic from each network interface based on preset rules

Network intrusion detection system (NDIS) alerts the administrator when it detects suspicious network traffic patterns

The slides are excerpted from Tilley 12 edition systems analysis and design book

Security Levels (6 of 12)

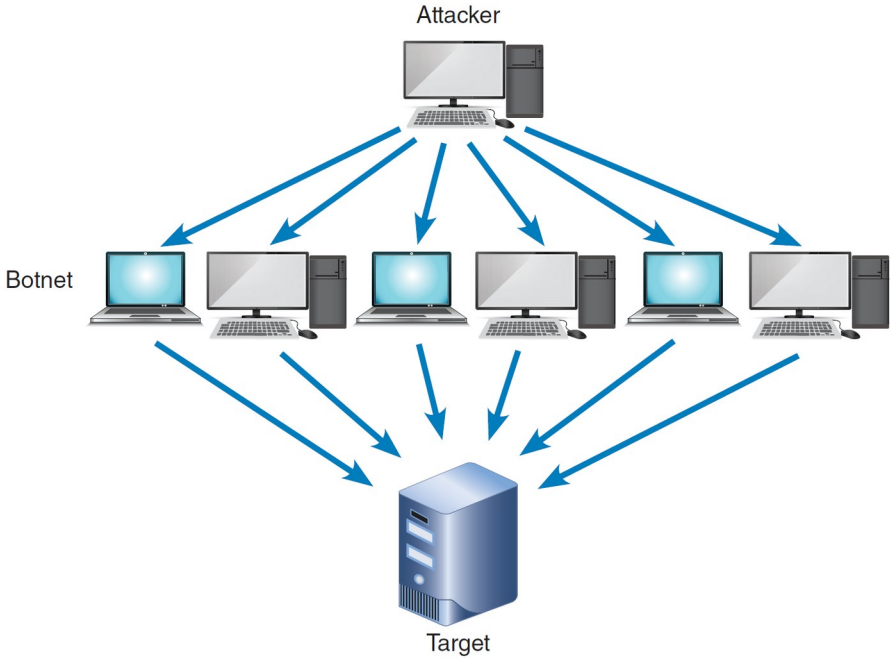
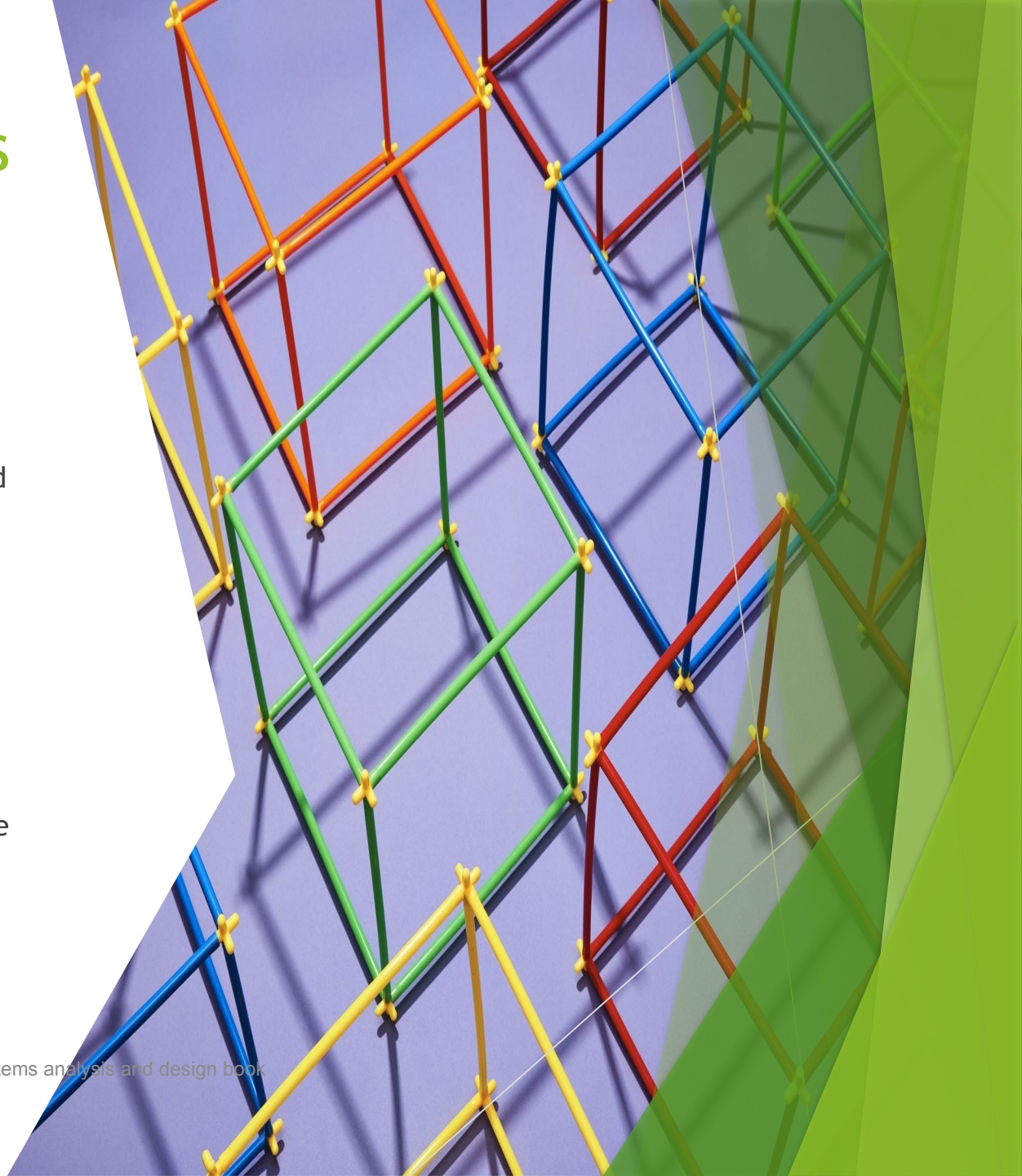


FIGURE 12-22: In a DoS attack, an attacker sends numerous authentication requests with false return addresses. The server tries unsuccessfully to send out authentication approval and is eventually disabled by the floor of requests. More sophisticated DoS attacks are distributed (DDoS), as shown in this figure. Instead of a single computer, the attacker uses an army of botnets (computers unknowingly infected with malware that are difficult to trace) to attack the target.

The slides are excerpted from Tilley 12 edition systems analysis and design book

Security Levels (7 of 12)



- Application security
  - Services that are not needed must be disabled
  - Unnecessary or improperly configured service could create a security hole
  - Hardening removes unnecessary accounts, services, and features
  - Application permissions: must be configured to be run by users who have specific rights
  - Input validation helps safeguard data integrity and security

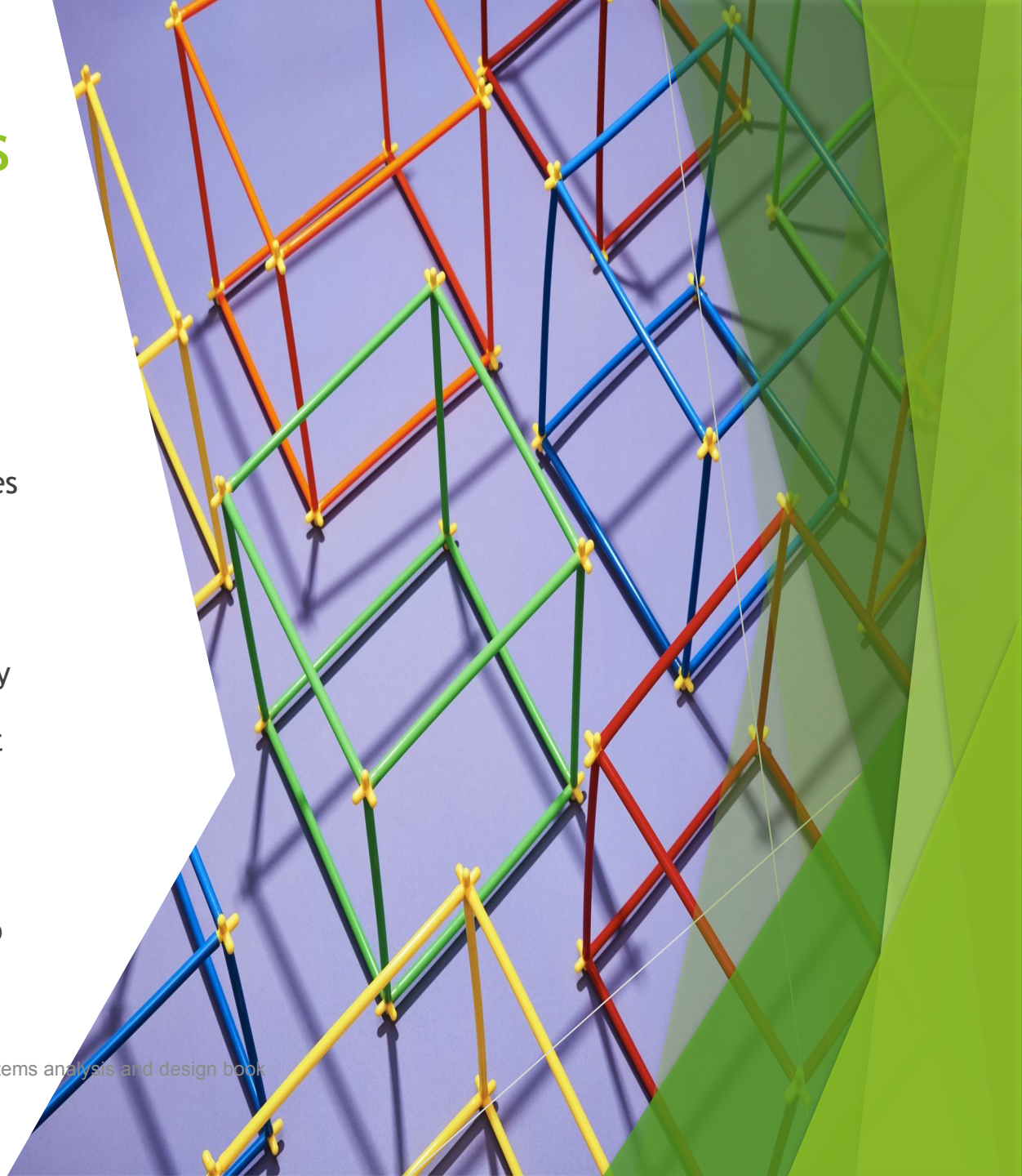
Security Levels (8 of 12)

- Patches and updates are used to repair security holes, reduce vulnerabilities, and update the system
- Software logs document all events and help understand past attacks and prevent future intrusions

Security Levels (9 of 12)

- File security
  - Encryption: scrambles the contents of a file or document to protect it from unauthorized access
  - Permissions: describe the rights a user has to a particular file or directory on a server
  - User groups: administrators can create user groups and assign file permissions

Security Levels (10 of 12)



- User security
  - Identity management: controls and procedures necessary to identify legitimate users and system components
  - Password protection: policies need to specify a set minimum length, complexity, and a limit on invalid attempts
  - Social engineering: intruder uses social interaction to gain unauthorized access to a computer system

Security Levels (11 of 12)

User resistance: users need to understand and be a part of the organization's commitment to security

New technologies can be used to enhance security and prevent unauthorized access

- Security token is a physical device that authenticates legitimate users

Security Levels (12 of 12)

- Procedural security (operational security)
  - Policies and controls that ensure secure operations
  - Defines how particular tasks are to be performed
  - Includes safeguarding procedures that would be valuable to an attacker
  - Organization must explain procedures and issue reminders that will make security issues a priority

The slides are excerpted from Tilley 12 edition systems analysis and design book

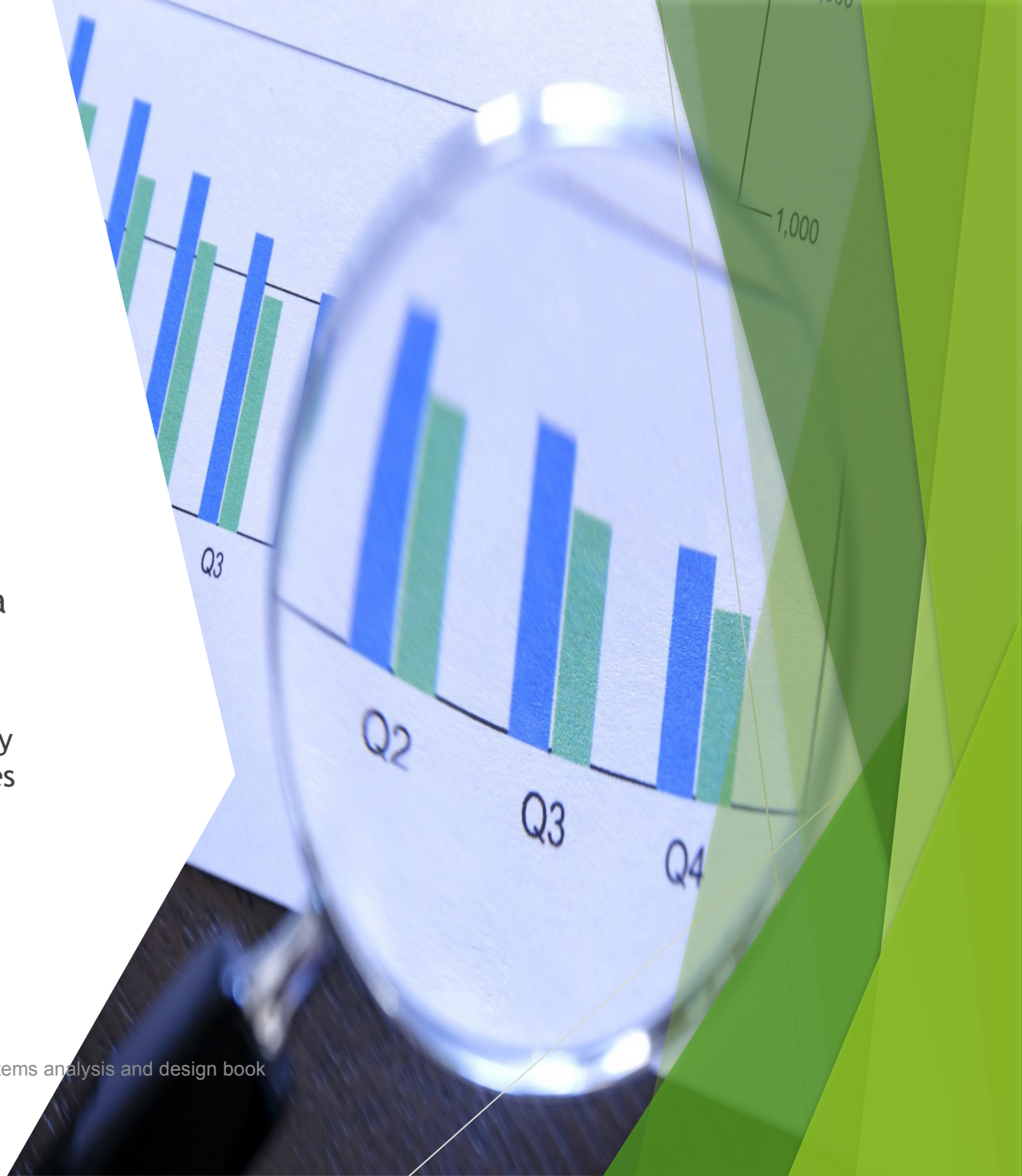
Backup and Recovery (1 of 2)

- Backup policies
  - Backup media: includes tape, hard drives optical and online storage
    - Offsiting: storing backup away from main location
    - Cloud-based storage is growing rapidly
  - Backup types: full, differential, incremental, and continuous
  - Retention periods: backups are stored for a specific time beyond which they are either destroyed or reused

The slides are excerpted from Tilley 12 edition systems analysis and design book

Backup and Recovery (2 of 2)

- Business continuity issues
  - A disaster recovery plan should be created along with a test plan
    - Often part of a business continuity plan (BCP): defines how critical business functions can continue during a major disruption



System Retirement

- Factors
  - Maintenance increasing steadily
  - Operational costs or times increasing rapidly
  - Software package provides the same or additional services more efficiently
  - New technology offers a way to perform the same or additional functions more efficiently
  - Maintenance changes or additions are difficult and expensive to perform
  - Users request significant new features

Future Challenges and Opportunities (1 of 3)

- Trends and predictions
  - Cybercrime will increase significantly
  - Smartphones and tablets will become the dominant computing platform
  - Software-as-a-Service will become the norm
  - Cloud computing will become the principal computing infrastructure
  - Insourcing will increase
  - Large enterprises may require suppliers to certify green credentials and sourcing policies

Future Challenges and Opportunities (2 of 3)

Strategic planning for IT professionals

System analysts should work backwards from goals to develop intermediate milestones

IT credentials and certification

Professional organizations and IT industry leaders offer continuing educational courses and credentialed certifications

Critical thinking skills

System analysts should possess soft skills and critical thinking skills

The slides are excerpted from Tilley 12 edition systems analysis and design book

Future Challenges and Opportunities (3 of 3)

- Cyberethics
  - As computers permeate more and more of our lives, the decisions made by IT professionals can have serious implications
  - Situations may arise involving ethical considerations that are not easy to resolve
  - Ethical, social, and legal aspects of IT are topics that today's systems analyst should be prepared to address

Summary (1 of 3)

Systems support and security	Types of system maintenance	Maintenance team
• Implementation of an information system until the system no longer is used	• Corrective, adaptive, perfective and preventative	• Systems analysts and programmers

Summary (2 of 3)

Configuration management and system performance measurements

- Necessities of maintenance management

Security is a vital part of every computer system

- Risk management identifies, analyzes, anticipates and reduces risk to an acceptable level
- Data backup and recovery plans are essential

Summary (3 of 3)

All information systems eventually become obsolete

Intense competition is predicted in the future

IT professionals should have a strategic career plan

Long-term goals

Intermediate milestones

The slides are excerpted from Tilley 12 edition systems analysis and design book