Securing Information System

Hello!

Name of Groups :

- Anggita Purbo Utami 16808144007
- Galih Prihanti 16808141005
- Rizka Nugraheni16808144024
- Luthfi Azis S P 16808144037
- Erlianti Indah B 16808141056

Why are information systems vulnerable to destruction, error, and abuse?

Can you imagine what would happen if you tried to link to the Internet without a firewall or antivirus software?

1.Why systems are Vulnerable

- Internet vulnerability
- Wireless security challenge

2. maliCious soFtWare: Viruses, Worms, trojan horses, and spyWare

- Malicious software programs are referred to as malware and cover various threats such as computer viruses, worms, and Trojan horses

3. haCkers and Computer Crime A hacker

- spoofing and sniffing
- denial-of-service attacks
- Computer Crime
- identity theft
- Click Fraud
- Global threats: Cyberterrorism and Cyberwarfare

4. internal threats: employees

- Employees have access to privileged information, and in the face of innate internal security procedures, they can often roam across an organization's system without leaving a trace.

5. soFtWare Vulnerability

- Software errors pose a constant threat to information systems, causing untold losses in productivity and sometimes harm to people who use or depend on the system.

What is the business value of security and control?_

1. leGal and reGulatory requirements For eleCtroniC reCords manaGement_

companies must take security and take more serious control by mandating data protection from unauthorized use, exposure and access. The Company faces new legal obligations for storage and storage of electronic records as well as for privacy protection.

2. eleCtroniC eVidenCe and Computer ForensiCsx0000 _

companies must take security and take more serious control by mandating data protection from unauthorized use, exposure and access. The Company faces new legal obligations for storage and storage of electronic records as well as for privacy protection.

What are the components of an organizational framework for security and control?

1. Information System Control

- General controls

  govern the design, security, and use of computer programs and the security of data files in general throughout the organization's information technology infrastructure

- Application controls

➢ *Input controls*

➢ *Processing controls*

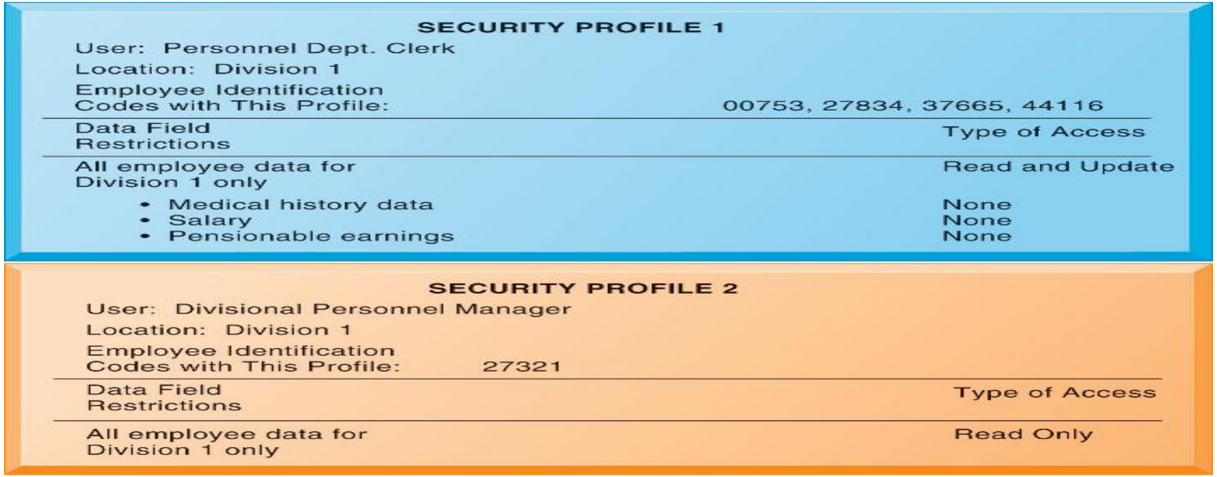
➢ *Output controls ensure*

2, Risk Assessment

- A risk assessment determines the level of risk to the firm if a specific activity or process is not properly controlled.

3. Security Police

After you've identified the main risks to your systems, your company will need to develop a security policy for protecting the company's assets.



SECURITY PROFILE 1

User: Personnel Dept. Clerk

Location: Division 1

Employee Identification Codes with This Profile: 00753, 27834, 37665, 44116

Data Field Restrictions	Type of Access
All employee data for Division 1 only	Read and Update
• Medical history data	None
• Salary	None
• Pensionable earnings	None

SECURITY PROFILE 2

User: Divisional Personnel Manager

Location: Division 1

Employee Identification Codes with This Profile: 27321

Data Field Restrictions	Type of Access
All employee data for Division 1 only	Read Only

4. Disaster recovery planning and business continuity planning

- **Disaster recovery planning** devises plans for the restoration of disrupted computing and communications services.
- **Business continuity planning** focuses on how the company can restore business operations after a disaster strikes.

5. The role of auditing

- How does management know that information systems security and controls are effective? To answer this question, organizations must conduct comprehensive and systematic audits.

What are the most important tools and technologies for safeguard information sources?

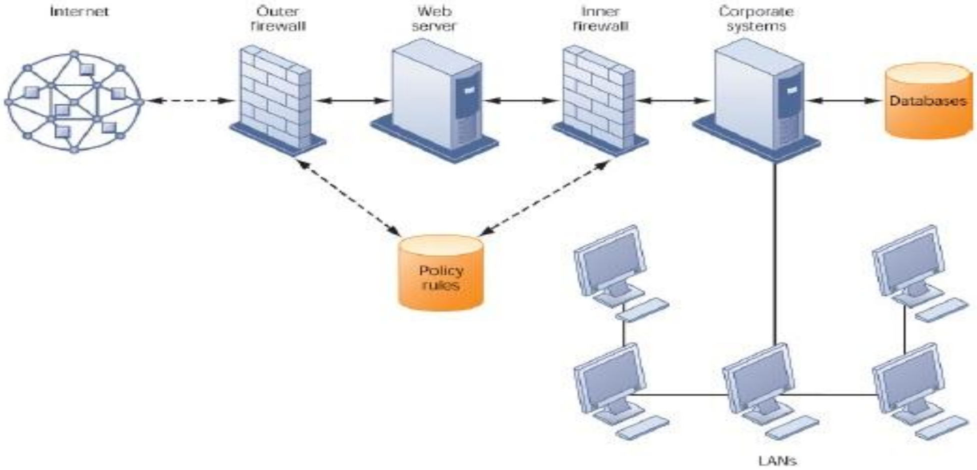
1. Identity Management and Authentication

- To gain access to a system, a user must be authorized and authenticated. **Authentication**refers to the ability to know that a person is who he or she claims to be. Authentication isoften established by using **passwords** known only to authorized users.

2. Firewalls, Instrusion Detection Systems, and Antivirus Software Firewalls

- **Firewalls** prevent unauthorized users from accessing private networks. A firewall is acombination of hardware and software that controls the flow of incoming and outgoingnetwork traffic.

Pict of A firewall is acombination of hardware and software that controls the flow of incoming and outgoingnetwork traffic.



•Packet filtering
•Stateful inspection
•Network Address Translation (NAT)
•Application proxy filtering
examines

3, Intrusion Detection System

- feature full-time monitoringtools placed at the most vulnerable points or hot spots of corporate networksto detect and deter intruders continually.

- ## 4. Antivirus and Antispyware Software

- prevents, detects, and removesmalware, including computer viruses, computer worms, Trojan horses, spyware, andadware

5. Unified Threat Management System

- To help businesses reduce costs and improve manageability, security vendors havecombined into a single appliance various security tools, including firewalls, virtualprivate networks, intrusion detection systems, and web content filtering and antispamsoftware.

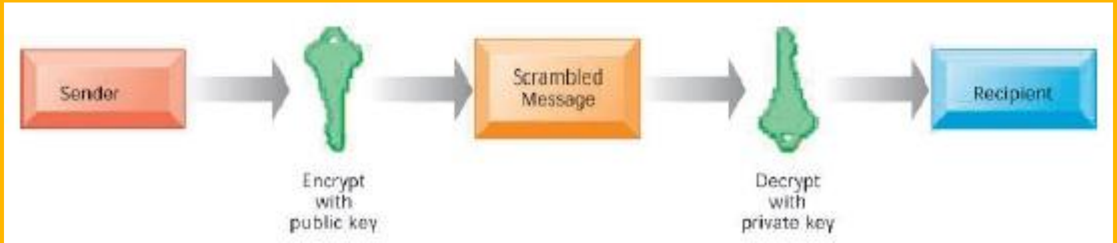
Securing Wireless Networks

- The initial security standard developed for Wi-Fi, called Wired Equivalent Privacy(WEP), is not very effective because its encryption keys are relatively easy to crack.

6. Encryption and Public Key infrastructure

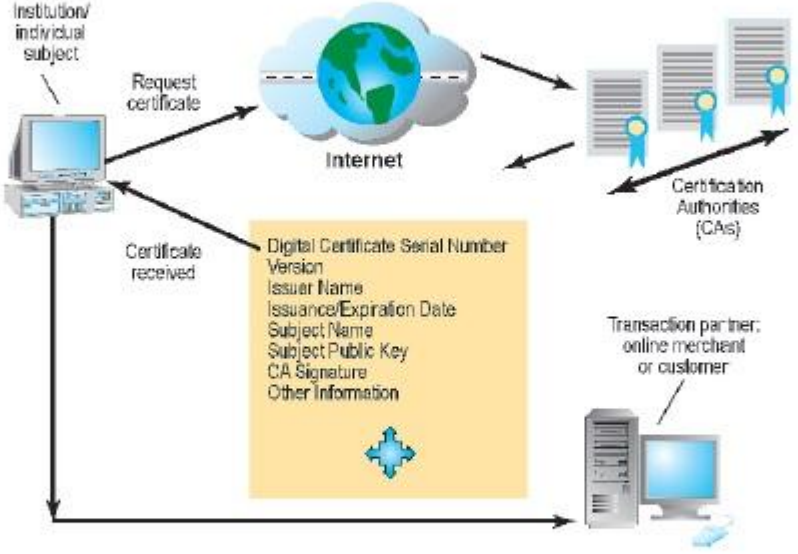
Encryption is the process of transformingplain text or data into cipher text that cannot be read by anyone other than the senderand the intended receiver. Data are encrypted by using a secret numerical code,

called an encryption key, that transforms plain data into cipher text. The messagemust be decrypted by the receiver.



Digital certificates

A digital certificatesystem uses a trusted third party, known as a certificate authority (CA), to validatea user’s identity.**Public key infrastructure (PKI)**, the use of public key cryptographyworking with a CA, is now widely used in e-commerce.



6. Ensuring System Availability

- Controlling Network Traffic: Deep Packet Inspection DPIexamines data files and sorts out low-priority online material while assigning higherpriority to business-critical files.

7. Security Outsourcing

- Many companies, especially small businesses, lack the resources or expertise to providea secure high-availability computing environment on their own.

8. Security Issues for Cloud Computing and The Mobile Digital Platform Security in the cloud

- Cloud computing is highly distributed. Cloud applications reside in large remotedata centers and server farms that supply business services and data managementfor multiple corporate clients. To save money and keep costslow,cloudcomputingproviders often distribute work to data centers around the globe where work can beaccomplished most efficiently. When you use the cloud, you maynot know preciselywhere your data are being hosted.

- ## 9. Securing Mobile Platform

- Mobile devices accessing corporate systems and data require special protection.Companies should make sure that their corporate security policy includes mobiledevices, with additional details on how mobile devices should be supported, protected,and used.

Thanks!

Any questions?