

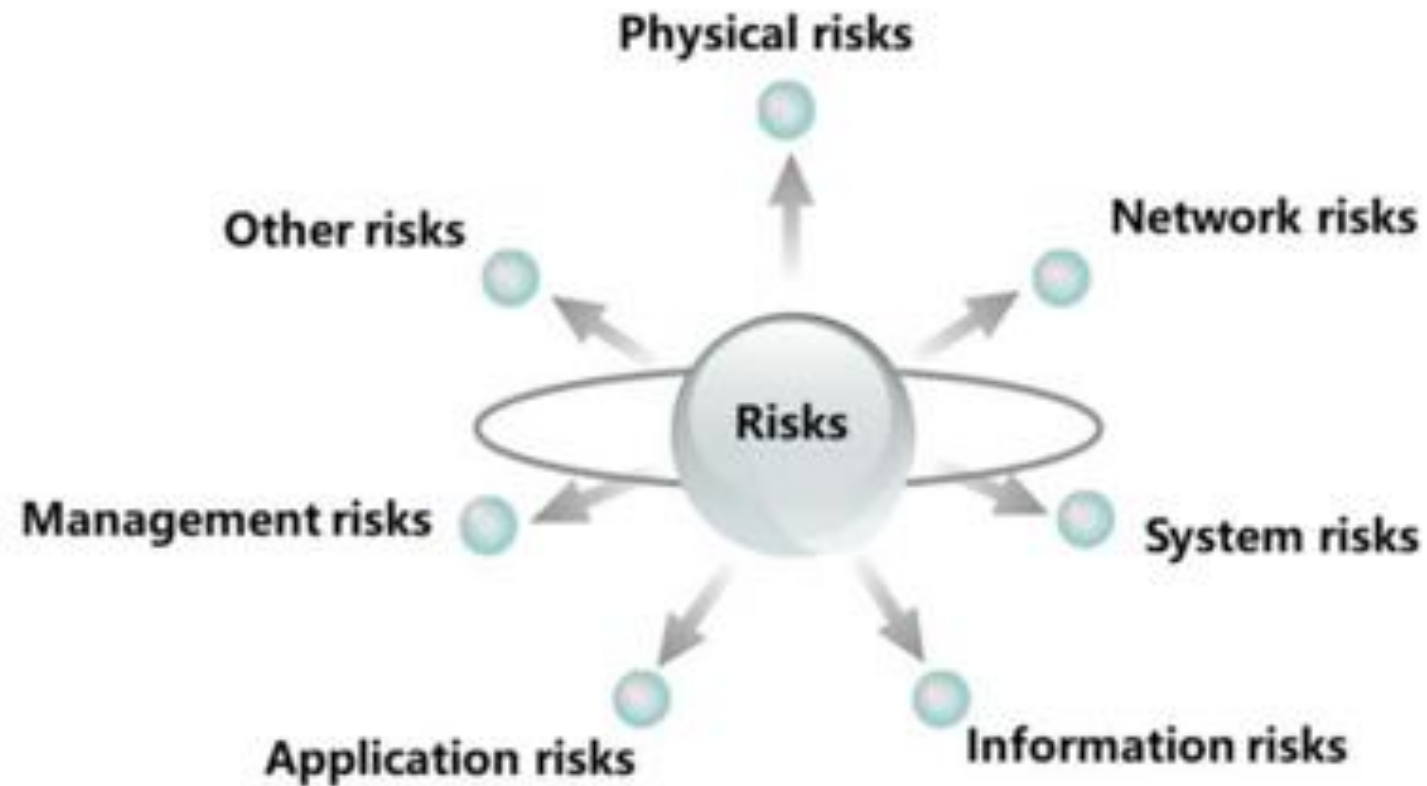
Information Security & Management

Lecture 1

HCIA-Security

Prepared by
Dr. Abdelrhman Ahmed

Risks Involved in Information Security



Physical Risks

- **Device theft and destruction**
- **Link aging, man-made damage, and bite from animals**
- **Network device fault**
- **Network device unavailability due to power failure**
- **Electromagnetic radiation in the equipment room**



Information Risks

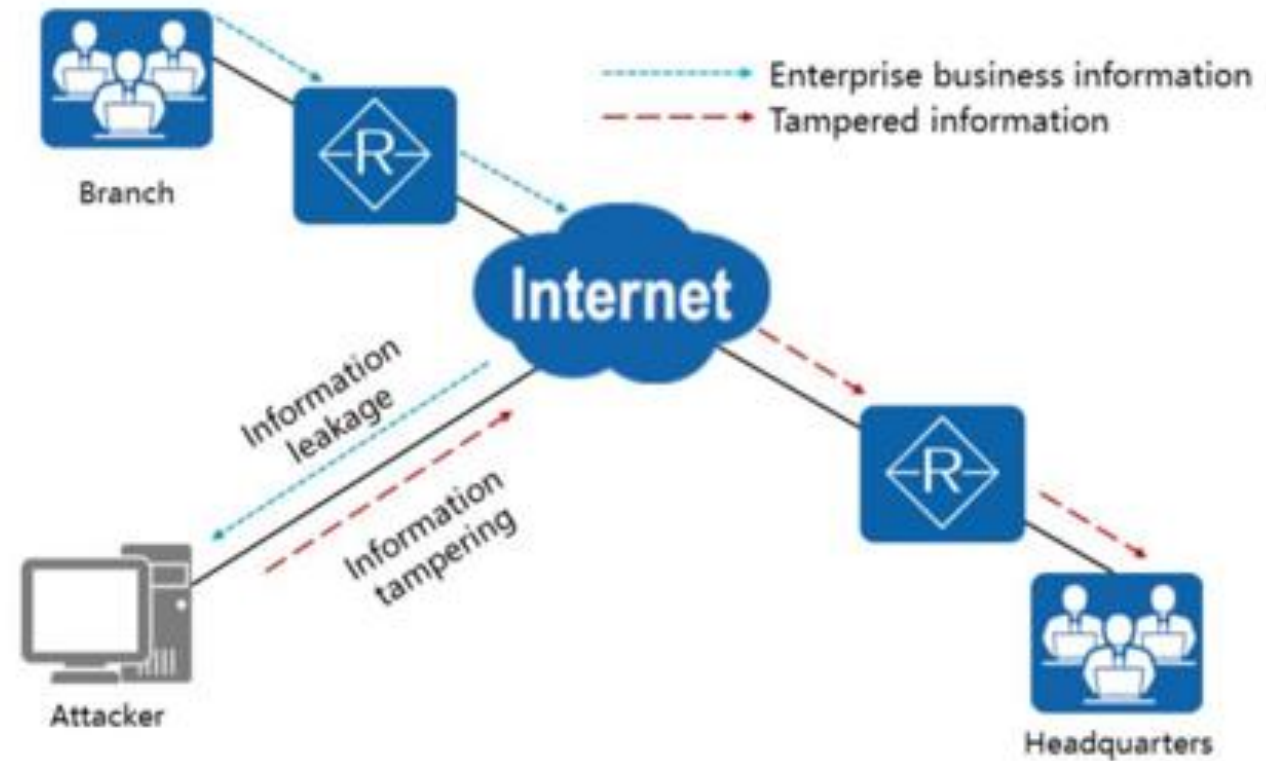
- **Information storage security includes protection of server disks and encryption and anti - theft of storage information.**
- **Storage security**
- **Transmission security**
- **Access security**



Information Transmission Security

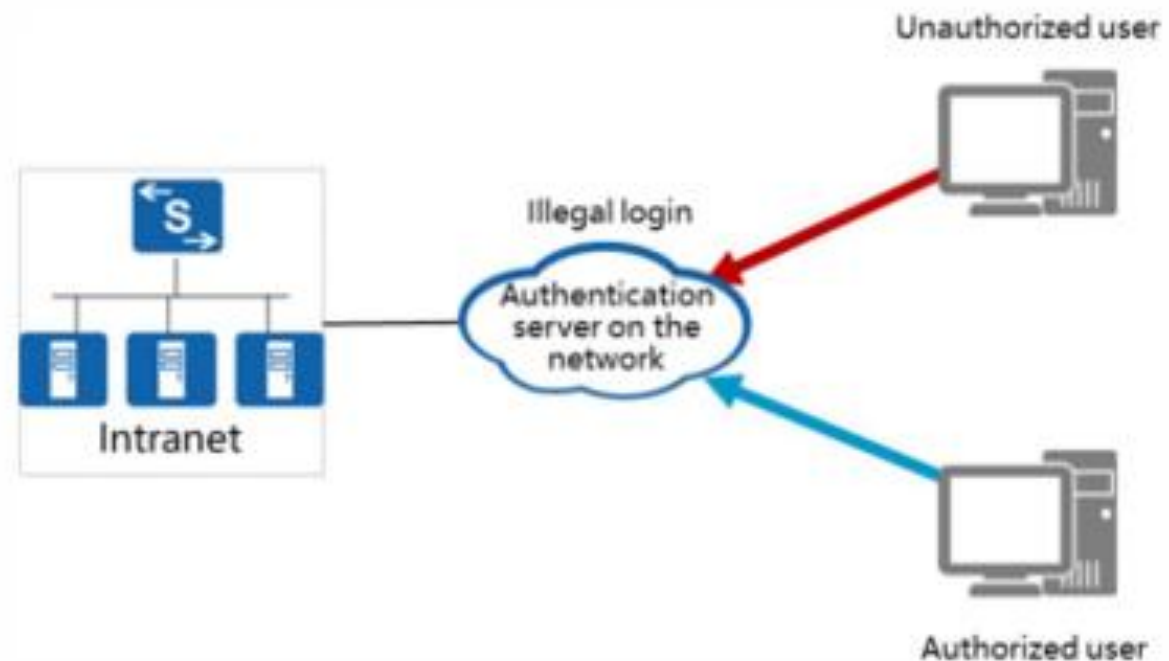
- The enterprise business information transmitted between the headquarters and branch may be stolen by the attacker.

In the figure, the attacker tampers with information sent by the branch, and then sends it on to the headquarters.



Information Access Security

- An unauthorized user impersonates an authorized user to remotely access intranet resources.



System Risks

- **Database system configuration security**
- **Security database**
- **Security of services running in the system**



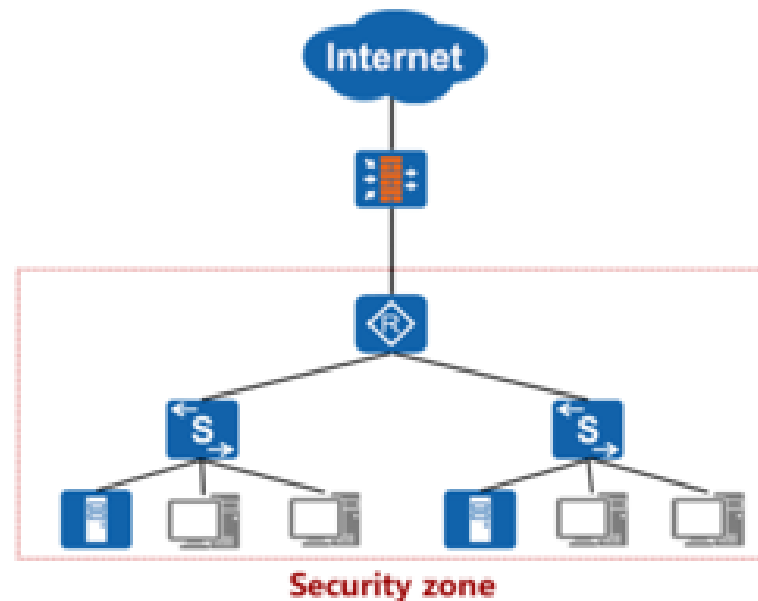
Application Risks

- Network virus
- Operating system security
- Email application security
- Web service security
- FTP service security
- DNS service security
- Business application software security



Network Risks

- **Security zone:** A network system generally has zones at different security levels, for example, a server zone at high security level and an office zone at low security level. Devices are placed in zones corresponding to their security levels, and untrusted zones are separated from security zones.



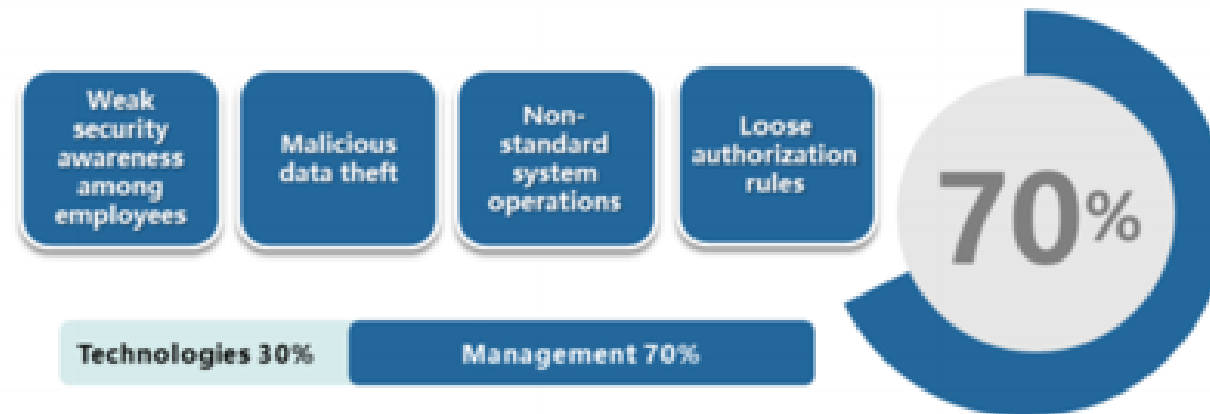
Management Risks

Determine whether the information system has management risks from the following aspects:



Significance of Information Security Management

- ❖ According to statistics, 70% of enterprise information loss is caused by negligence or intentional leakage by internal staff.



- ❖ Security technologies are only the means to control information security. They can only be effective with the appropriate support of management procedures.
- ❖ Effective management is an essential part of achieving information security goals. Its role should not be underestimated.

Current Development of Information Security



Introducing information security development strategies and plans

Each country has introduced its own information security development strategy and plan.



Strengthening legislation to achieve unified and standardized management

Defining and standardizing information security work through laws is the strongest guarantee for effective implementation of security measures.



Entering the era of standardized and systematized management

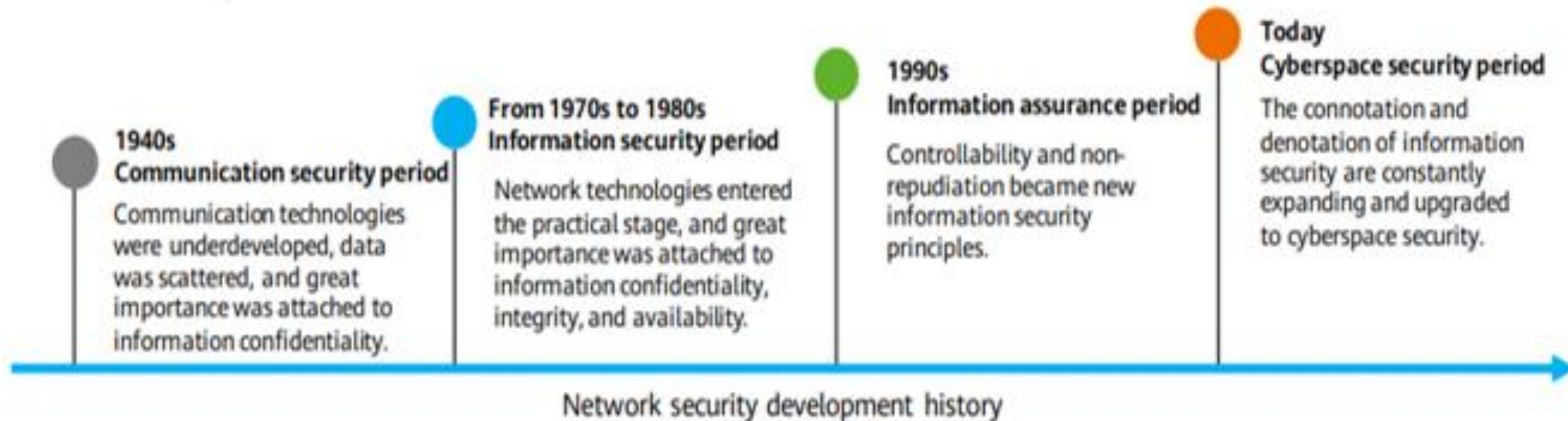
The era of standardized and systematized information security management began in the 1990s. ISO/IEC 27000 is the best known system.

Cybersecurity

Network security refers to cybersecurity, which is cyberspace security at a national level. Cyberspace consists of separate and interdependent information infrastructure and networks, including the Internet, telecom networks, computer systems, and embedded processors and controllers

In a narrow sense, network security generally refers to taking necessary measures to prevent attacks, intrusions, interference, damage, and unauthorized use of networks and information transmitted over networks, as well as unexpected accidents, to help networks run in a stable and reliable state and ensure the integrity, confidentiality and availability of network information and data.

Network Security Definition



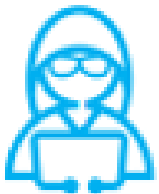
Communication Security Period

In the 1940s, communication technologies were underdeveloped, and data was stored in different locations. Information system security was limited to physical security of information and cipher-based security of communication (mainly stream cipher).

For example, information was stored in a relatively secure place, and unauthorized users were prohibited from accessing the information; cryptographic technologies were used to ensure the security of different information exchange processes such as telephone, telegraph, and fax, thereby ensuring data security.

It was crucial to ensure data security during transmission between two locations.

Network Security Threats



Hackers are the initiators of information security incidents. They attack networks to obtain useful information or substantial rewards, which is usually accompanied by criminal acts.



Vulnerabilities are the root cause of all security problems. New vulnerabilities increase rapidly, while vulnerability discovery penetrates from the application layer to bottom-layer components, and even to the architecture layer, expanding the impact.

Network Security Threats



The number of **ransomware attacks** continues to grow. As the attack threshold is lowered, multiple ransom policies may become the attack mainstream. The requested ransom becomes higher, and phishing and remote desktop protocols are the main media of ransomware attacks.



DDoS attacks are becoming a service and a new means for attackers to gain profits. Attackers obtain economic benefits by selling cybercrime toolkits and services, and cybercrime is rising.



Thank You