# Basic Concepts of Information Security

www.huawei.com



HUAWEI

# Foreword

- Information security is the process of ensuring safe data communication and preventing issues such as information leakage, modification, and disruption.
- This document describes the basic concepts and protection measures of information security, as well as information security risks and associated assessment and avoidance methods.

# Objectives

- Upon completion of this course, you will be able to:
  - Describe the definition and characteristics of information security.
  - Explain the characteristics and differences of security models.
  - Differentiate between security risks.

# Contents

# Information

**What is information?**

- Books/ Letters
- State secrets
- Emails
- Radar signals
- Transaction data
- Test questions

- information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business.

--- ISO/IEC Guidelines for the Management of IT Security (GMITS)





- Information can be communicated in a number of different ways: messages, signals, data, intelligence, or knowledge. It may exist in multiple forms, for example, data/programs stored and processed in information facilities, printed or written papers/emails/design drawings/business solutions, or messages in slides or sessions.

# Information Security

- Information security refers to the preservation of the confidentiality, integrity, and availability of data through security technologies.
- These technologies include computer software and hardware, network, and key technologies. Organizational management measures throughout the information lifecycle (generation, transmission, exchange, processing, and storage) are also essential.
- The following will be affected if information assets are damaged:

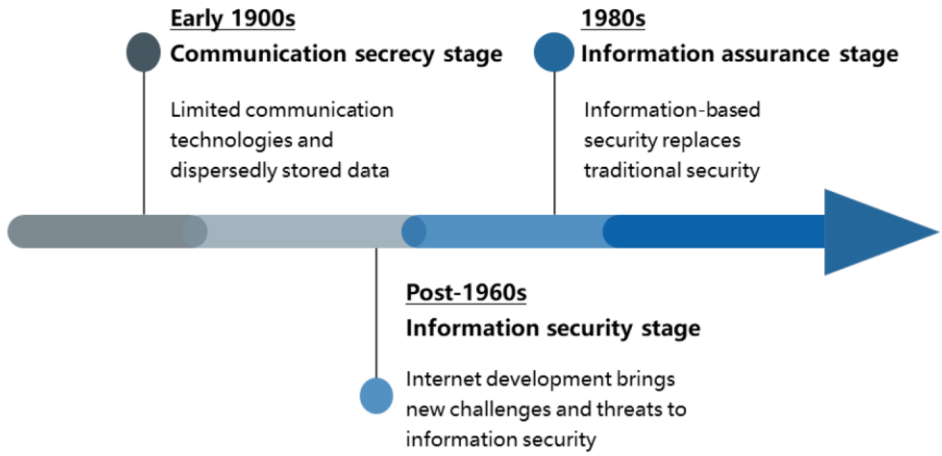

- The aim of information security is to protect data against threats through technical means and effective management.





- Information security is to protect hardware, software, and system data on information networks from occasional or malicious damage, tampering, and leakage. It ensures continuous and reliable system operating as well as uninterrupted information services.

# Information Security Development



# Photo or Information Leakage?

- After the Chinese government invited bids for oil production equipment, Japanese intelligence experts used this simple photo to uncover the following secrets of the Daqing Oilfield:
  - Located between 46°N and 48°N, as indicated by the clothing of Wang Jinxi
  - Diameter of the oil well, inferred from the handle rack

## Communication Secrecy Stage

- In the early 1900s, 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).
- As long as information was in a relatively secure place and unauthorized users were prohibited from accessing the information, data security could be generally guaranteed.





- In the case mentioned previously, it was ignored that the photo might reveal sensitive information about the oilfield. By limiting the dissemination or recipients of the photo, information leakage could have been prevented.

## Information Security Stage

- Since the 1990s, Internet technologies have developed rapidly, and information leaks have increased.
- As a result, in addition to confidentiality, integrity and availability, information security began to focus on more principles and objectives, such as controllability and non-repudiation.

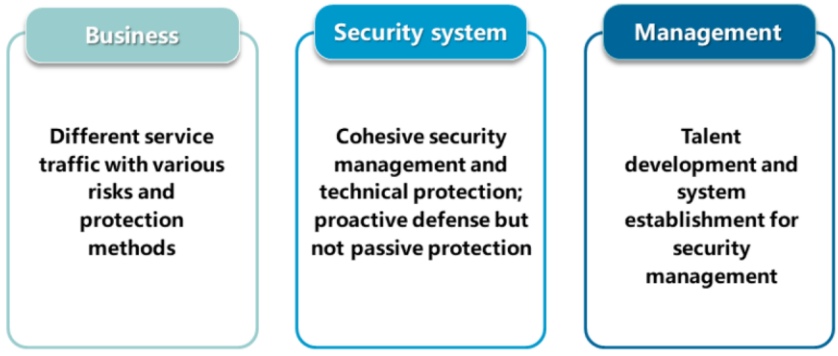





- Confidentiality
  - Ensures that information can be obtained only by authorized users.
- Integrity
  - Ensures the accuracy and integrity of information and its processing method.
- Availability
  - Ensures that authorized users can obtain desired information and use related assets.
- Controllability
  - Implements security monitoring to protect information and its system against attacks.
- Non-repudiation
  - Prevents the information sender or receiver from denying the information.
- Information security involves information confidentiality, integrity, availability, controllability, and non-repudiation. In general, information security is to ensure the effectiveness of electronic information. Confidentiality means resisting passive attacks by adversaries and preventing information leakage to unauthorized users. Integrity means resisting active attacks by adversaries and preventing unauthorized tampering. Availability is to ensure that information and information systems are actually used by authorized users. Controllability is to implement security monitoring on information and information systems.

# Information Assurance Stage

- Business-oriented information security assurance



# Case - WannaCry


- In 2017, the WannaCry ransomware cryptoworm, propagated through EternalBlue, infected over 100,000 computers, causing a loss of US$8 billion.



HUAWEI

- Exploiting the vulnerability of port 445 on Windows operating systems, the WannaCry ransomware cryptoworm featured self-replication and included a "transport" mechanism to automatically spread itself. Among infected Windows operating systems in China, those on campus networks suffered most, and a large number of laboratory data and final year projects were locked and encrypted. The application systems and database files of some large enterprises were encrypted and failed to run properly.

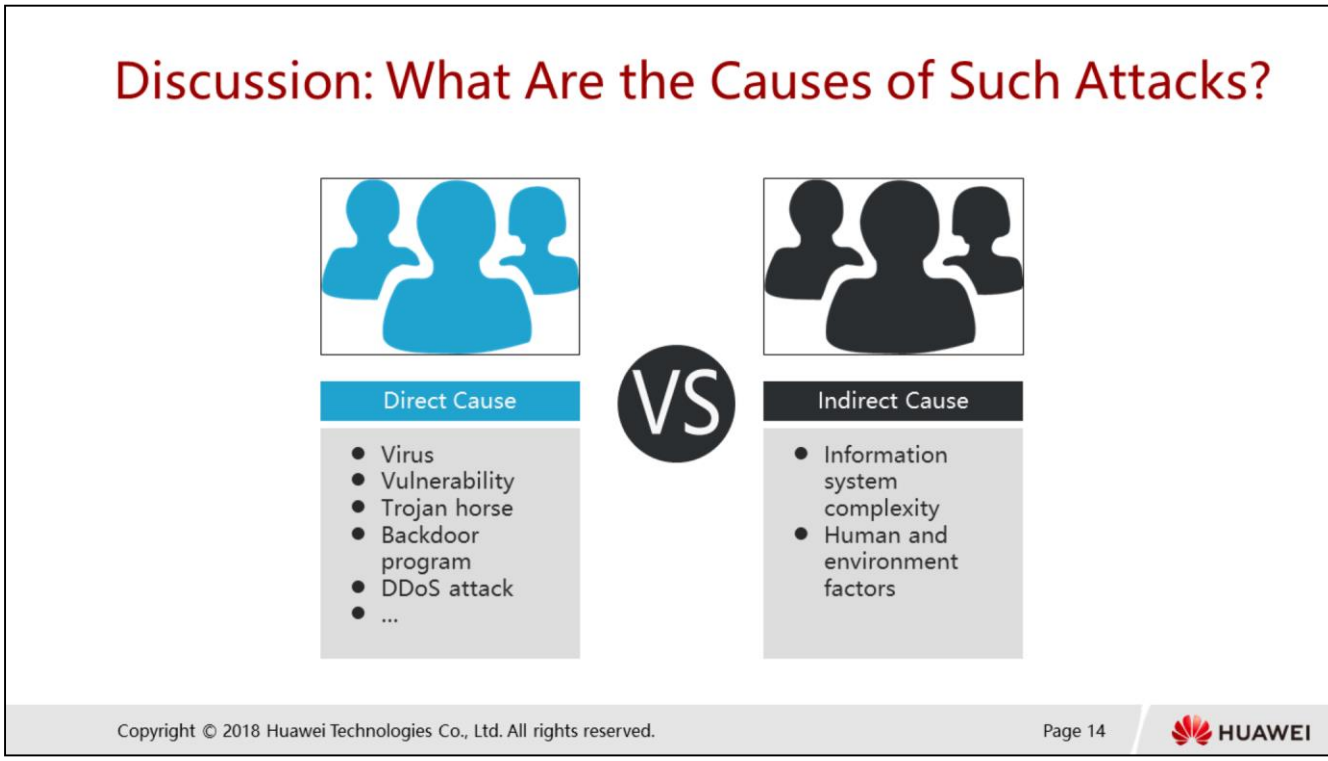
# Case - OceanLotus


- Since April 2012, the OceanLotus group has carried out targeted penetration and attacks on important sectors of China, such as the government, scientific research institutes, maritime institutions, maritime construction, and shipping enterprises.
- The attacks are intended to obtain confidential information, intercept intelligence sent out by attacked computers, and enable the computers to automatically send related intelligence.



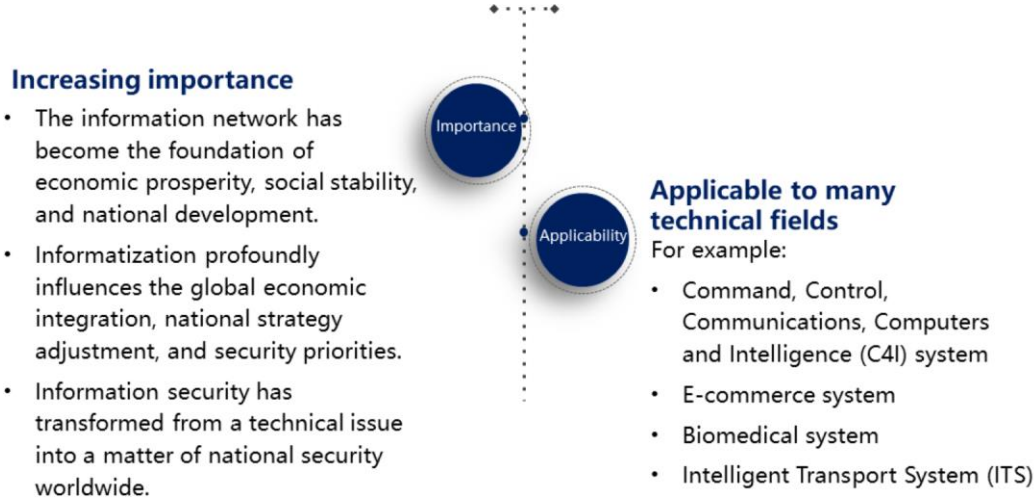
HUAWEI

- The OceanLotus group mainly uses two attack methods:
  - Spear phishing: The Trojan horse is emailed to targeted computers as an attachment with an attractive title (such as Salary Reform Scheme). The computers are infected after the attachment is opened.
  - Watering hole: The attacker exploits the vulnerabilities of websites that targeted individuals or organizations visit frequently and use these websites to distribute malware. For example, on the intranet server that employees frequently visit, the attacker replaces an internal shared document with the Trojan horse. All computers that download the document as required will be infected with the Trojan horse and send confidential information to the attacker.




- Information system complexity: The information system may be attacked during the design or operation process due to its vulnerabilities and defects. Major issues are as follows:
  - Complex process: In information system design, security is placed inferior to factors such as usability and enforceability. Due to human error and imperfect design methodology, the information system always has vulnerabilities.
  - Complex structure: The information system may need to support multiple types of terminals (such as employee terminals, remote users, mobile terminals, routing devices, and servers) and data services (such as service data, management data, and voice data) on the network. All terminal and data types must be considered for cyber security management.
  - Complex application: Network redundancy and stability are preferentially considered during network topology design, and redundant links and backup devices may be added. The complexity of network application can lead to failure in rapid fault locating and rectification.
- Human and environment factors: environmental threats and man-made damages.

# Significance of Building Information Security






HUAWEI

- Information security, in the broadest terms, defines data confidentiality, integrity, availability, controllability, and non-repudiation. In terms of cyber security, information security defines more specific requirements, such as physical security, identity authentication, and audit and monitoring.
- The C4I system is mainly used in the military field.

# Contents

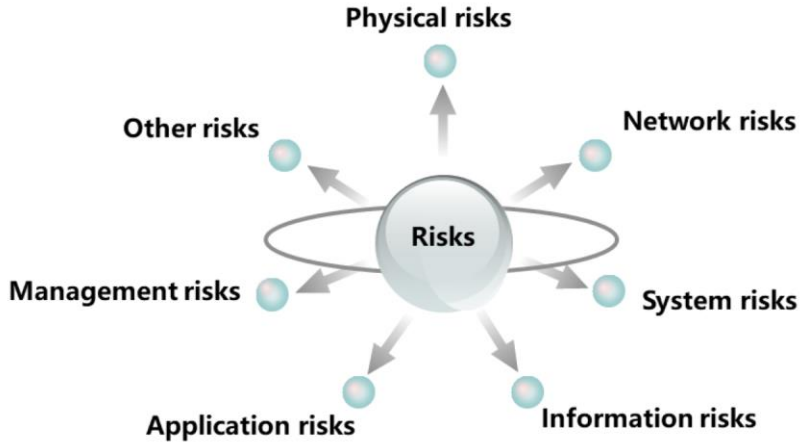






HUAWEI

# 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

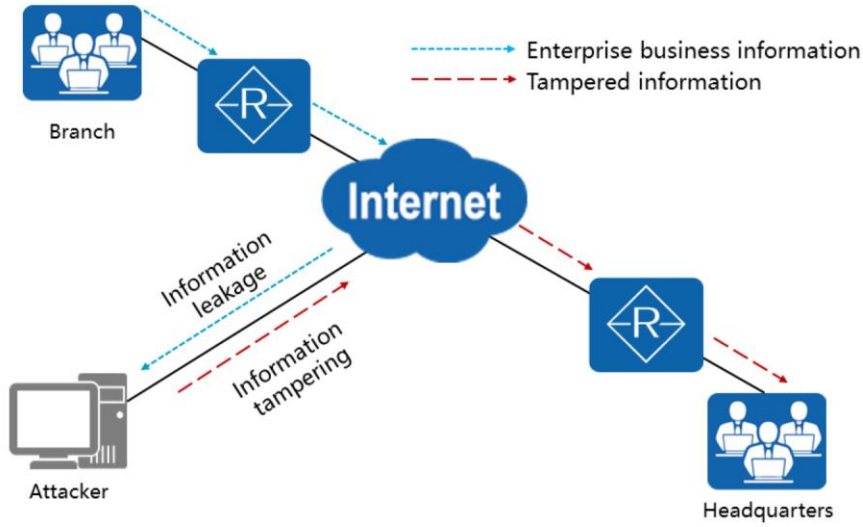
- Storage security
- Transmission security
- Access security





- Information storage security includes protection of server disks and encryption and anti-theft of storage information.

# Information Transmission Security

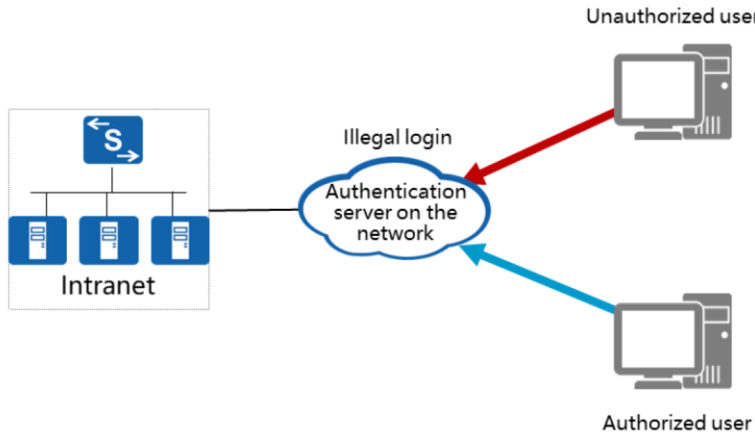





HUAWEI

- 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

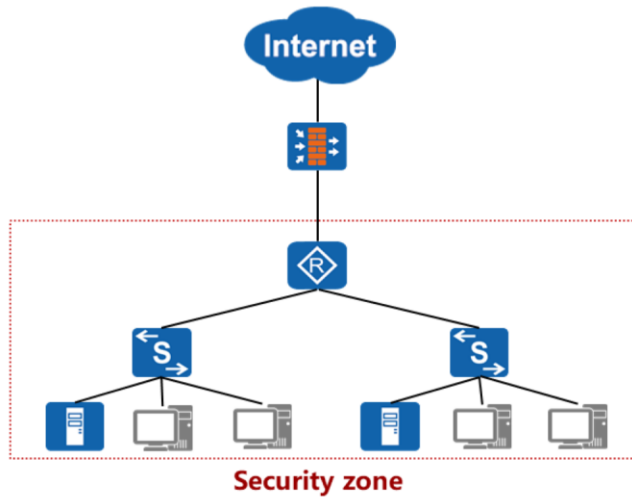
# Application Risks

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




HUAWEI

## 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

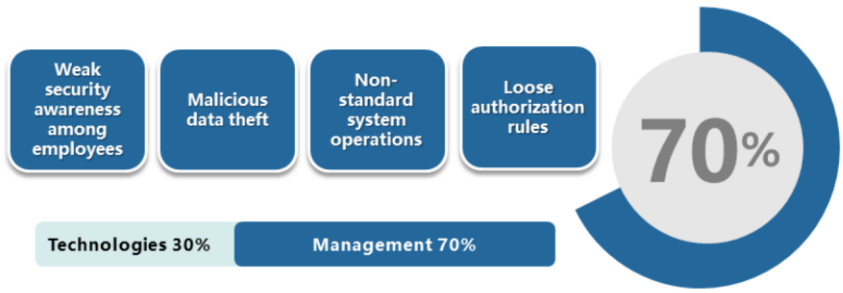
- Determine whether the information system has management risks from the following aspects:




HUAWEI

# 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.



HUAWEI

- Effective management is an essential part of achieving information security goals. Its role should not be underestimated.

# Current Development of Information Security Management


**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.