GALGOTIAS UNIVERSITY

School of Computer Science and Engineering

Course Code : BCSE 2380

Course Name :

CYBER SECURITY

Week 1: Introduction to Cyber Security – Cyberspace – Information Systems – Security Principles - Importance of Cyber Security

Module 3: Importance and Need for Cyber Security – Cyber threats – Cyber challenges

Course Co-Ordinator

Dr. Jayakumar .V

Assistant Professor

Department of Computer Science and Engineering
Galgotias University

Objectives

- ✓Justify the need for Cyber Security
- ✓Emphasis on Cyber Security Challenges

Learning Outcomes

- ✓Derive the important terminologies and difference between certain terms
- ✓Summarize and Illustrate the security rudiments through the incidents happened both at National and International Level
- ✓Outline and Prepare the fundamentals of Security Practices and Comprehend the Security Challenges

Outline

Why Cyber Security is important?
Who are Hackers? What do they do generally?
Common ways of how a computer can become infected
Statistics on Cyber Attacks
Need for Security- A Technological View
Types of Cyber threats
Attacks on Confidentiality
Attacks on Integrity
Attacks on Availability
Methods and Practices of Countering Cyber Attacks
Social Engineering
Phishing Attacks
Unpatched Software
Social Media Threats
Advanced Persistent Threats

Outline

Cyber Security Core Functions
Four Important Fundamentals of Security
Protect the Device
Protect the connection of Device
Protect Email Communication
Protect and backup electronic documents and files
Other essentials in securing the Computing systems
Physical Security
Protect against Unauthorized Administrators
Assign the least Permissions possible
Use the most secure Operating Systems possible
Use Strong passwords or Pass Phrases
Use Secure Authentication methods
Cyber Security Challenges

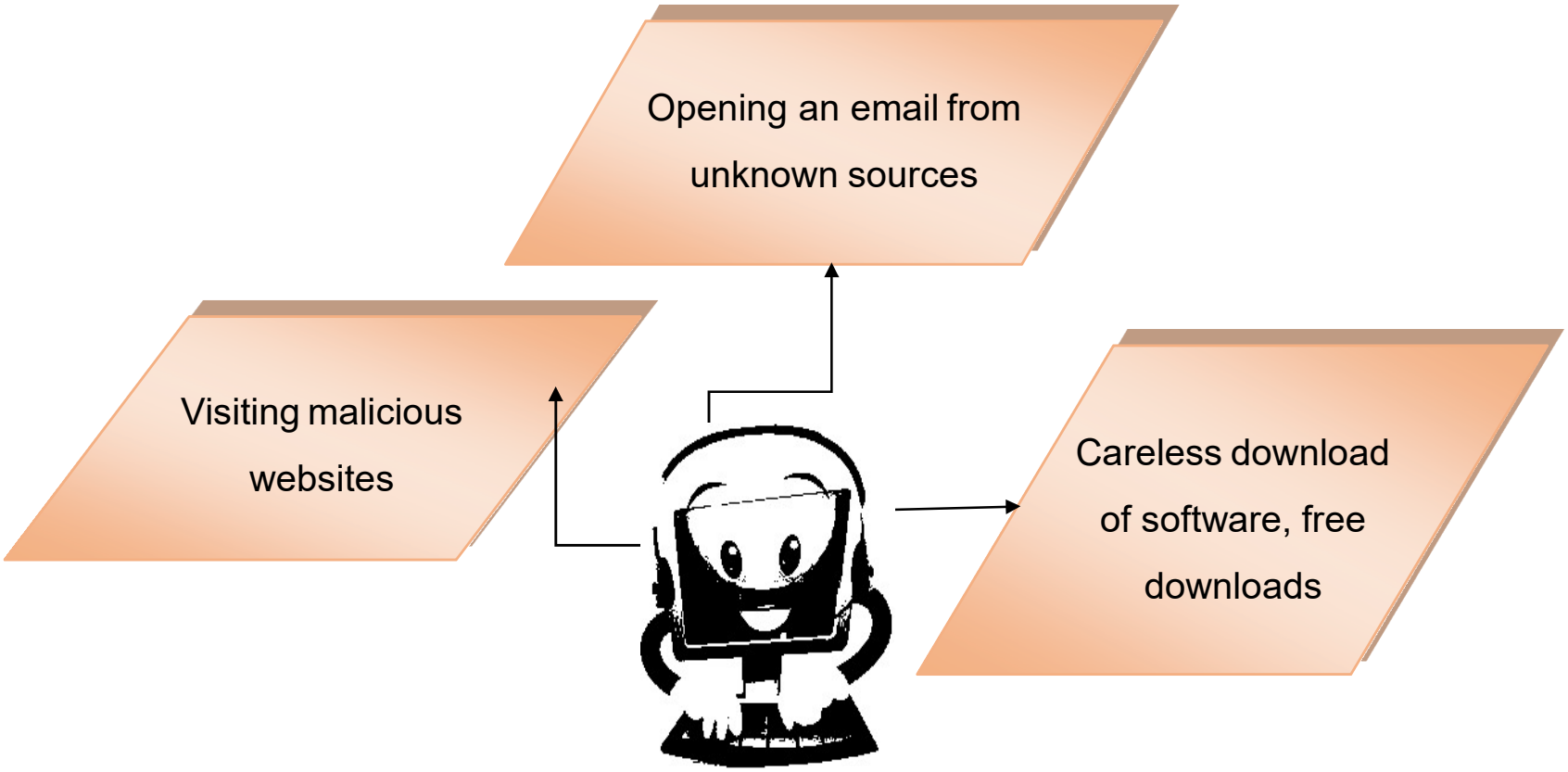
Why Cyber Security is important?

- Cyber Security is not a one-time process to achieve
- It is an ever growing challenge encountered from time to time
- When old problems are fixed and rectified, new targeted attacks challenge the Cyberspace
- Cyber security is a process by itself and not the end

Hackers

- Hackers are unauthorized users of a system
- They invade a system through the vulnerabilities or weak points in the system
- They makes use of large diverse tools to harm a computer system
- They gain access to computer systems through malicious logic

Common ways a computer can become infected



Top Five Risks- Global Instability

- According to the World Economic Forum's Global Risk Report 2018, Cyber-attacks are 3rd threat the World is facing today after natural disasters

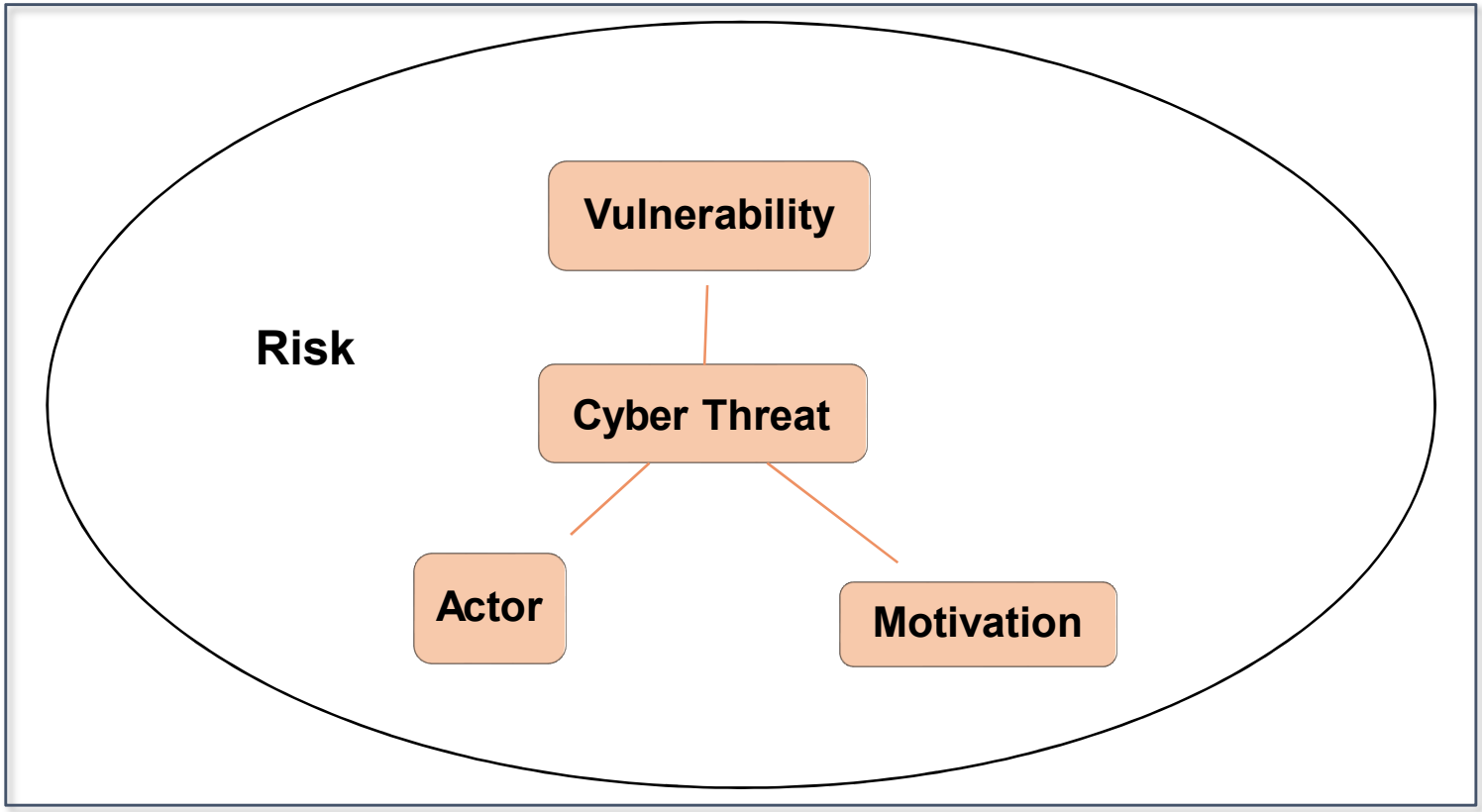
Cyber Attacks in the Year 2018

- WannaCry ransomware, Petya, and NotPetya led to $300 million loss in companies
- The ransomware spread through emails demanded money for release of encrypted data
- Billions of data records are leaked for Business & Political gains

Important Terminologies

- **Vulnerability –** any weakness in the system
- **Threat –** possible danger to assets
- **Attack –** evades security services and violates security policy
- **Risk –** possibility of suffering loss

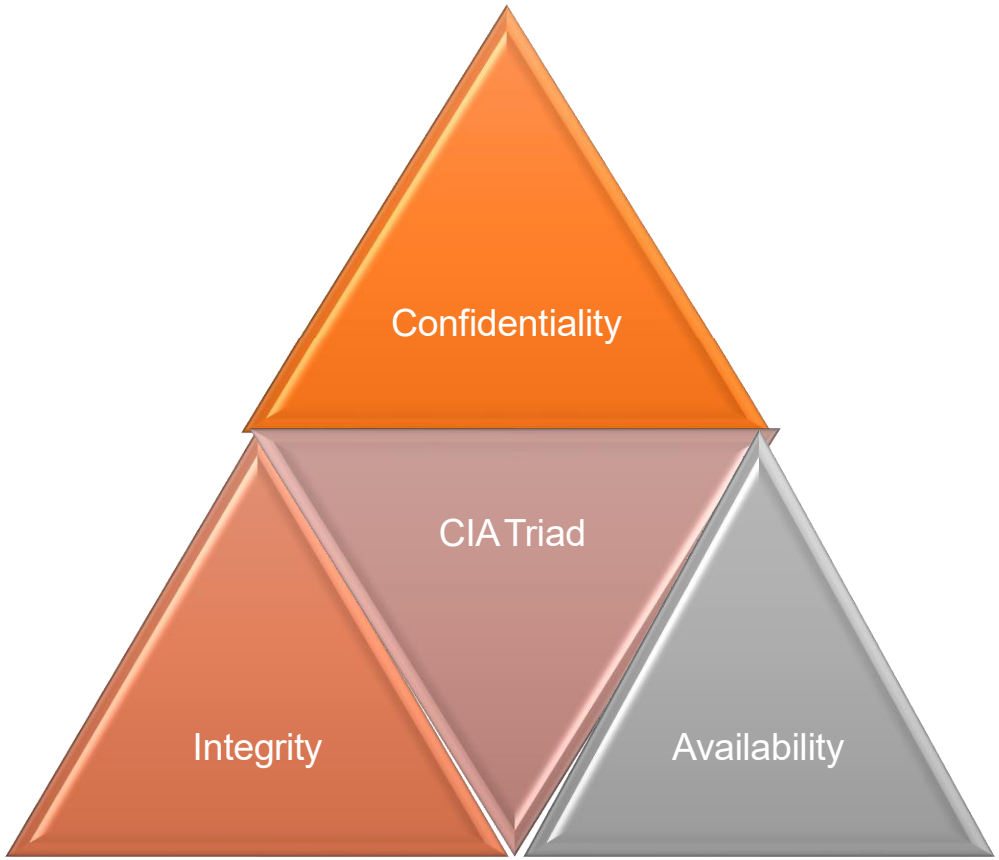
Interdependency of vulnerability, threat and risk



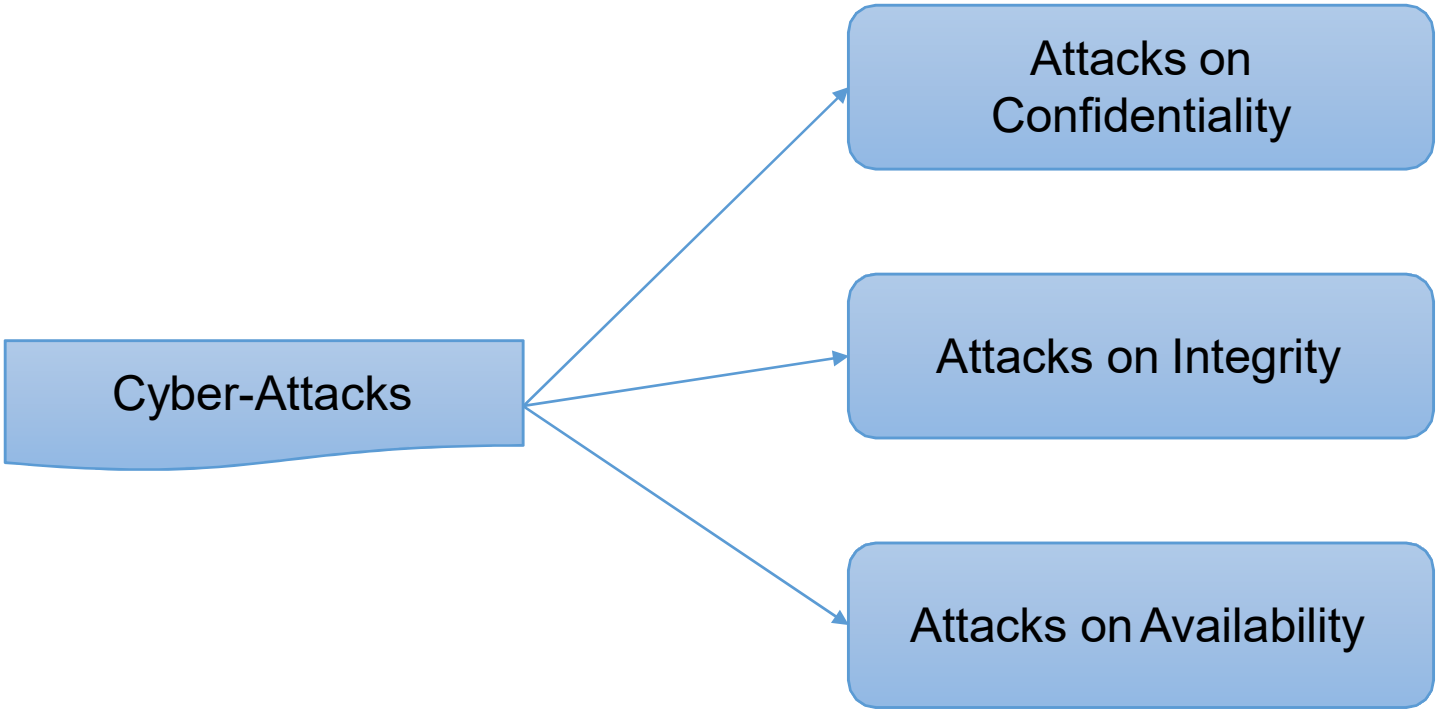
Types of cyber threats

- An actor of adversary gains access to the system in a number of ways
- Threats gains access to networks through malicious attempts
- The types of threats are increasing in its landscape by two technology trends
  - IoT (Internet of Things) and
  - Data Proliferation

CIA Triad



Common categories of Cyber-attacks



Attacks on confidentiality

- Stealing or copying the target's personal information
- For example, attacks like credit card fraud, identity theft, or stealing bitcoin wallets
- Carried out for political, military, or economic gains

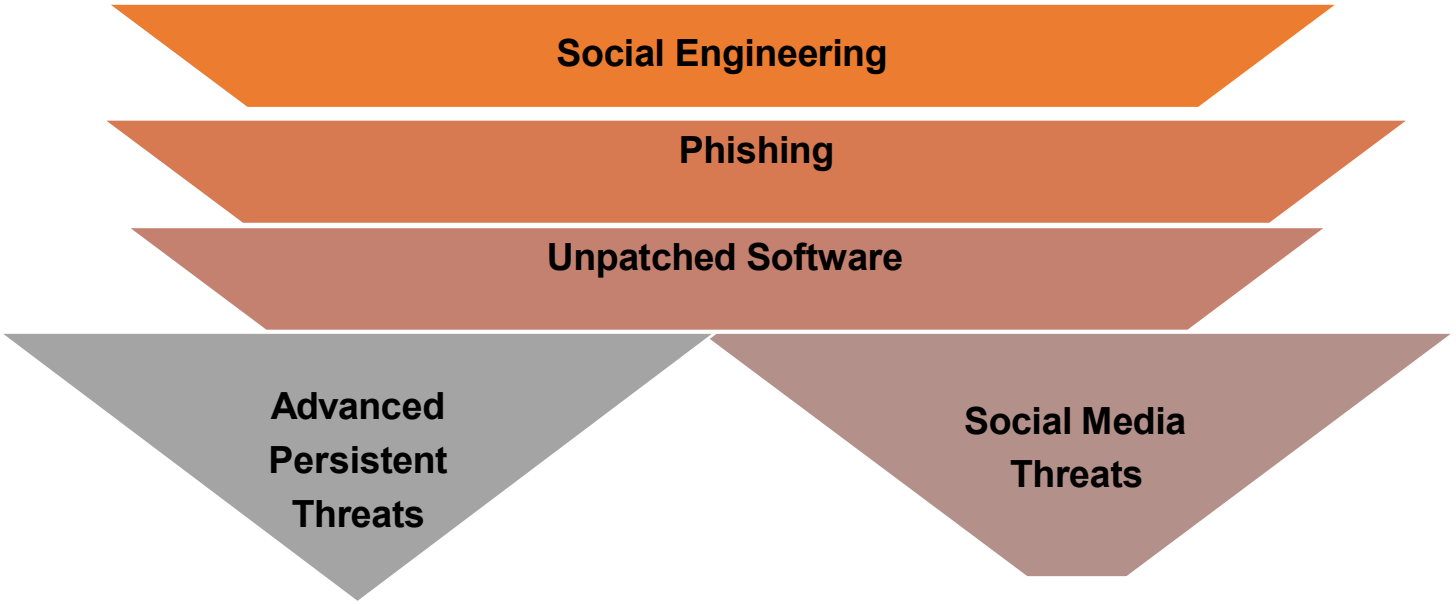
Attacks on integrity

- The common name used is sabotage
- Seeks to corrupt, damage, or destroy information or systems
- Offenders can range from script kiddies to international or national attackers

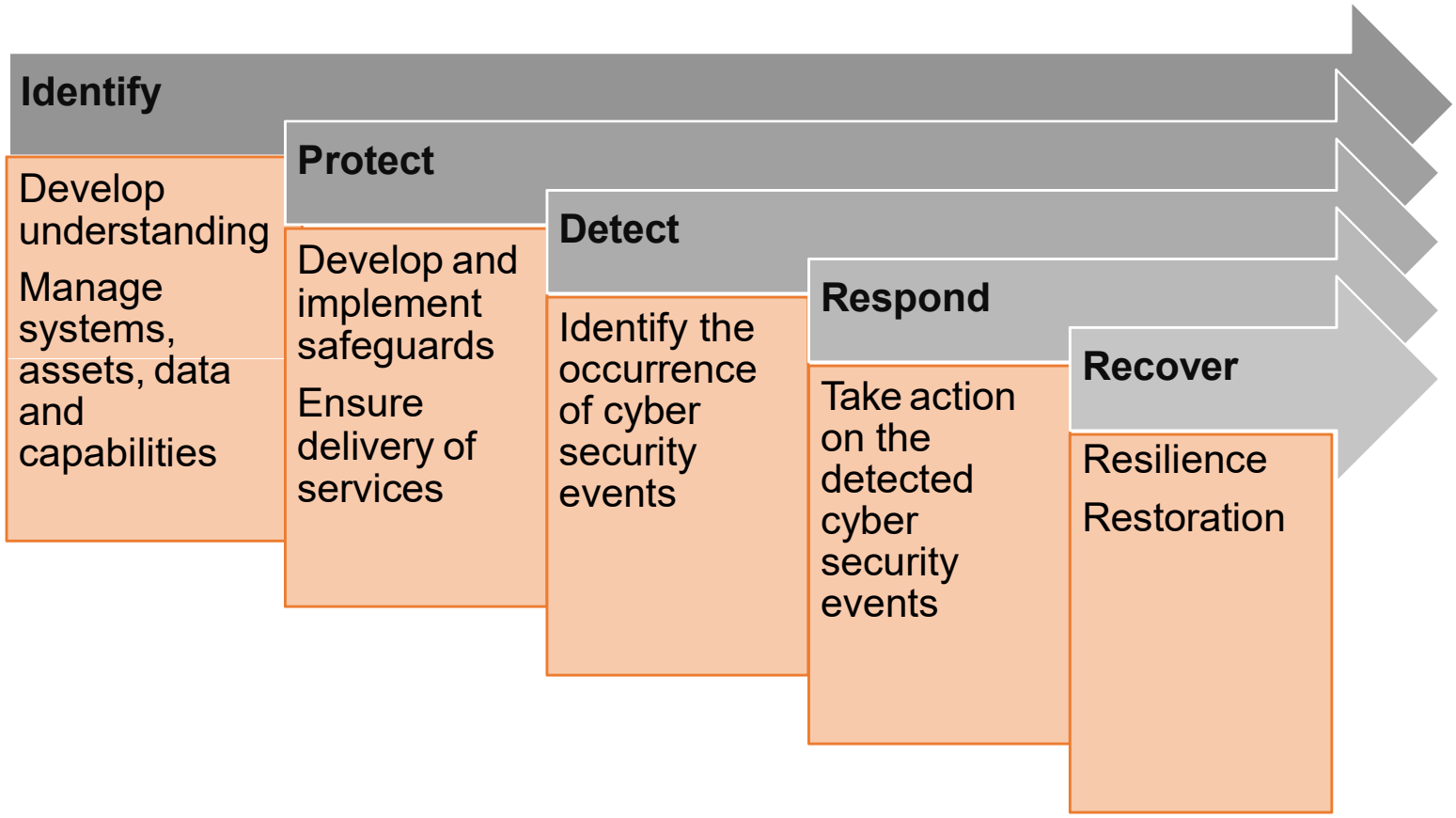
Attacks on availability

- Preventing a target from accessing by the genuine users
- For example, ransomware and denial-of-service attacks
- Ransomware encrypts the target's data and demands a ransom to decrypt it
- DoS floods a network resource with requests, making it unavailable due to jam

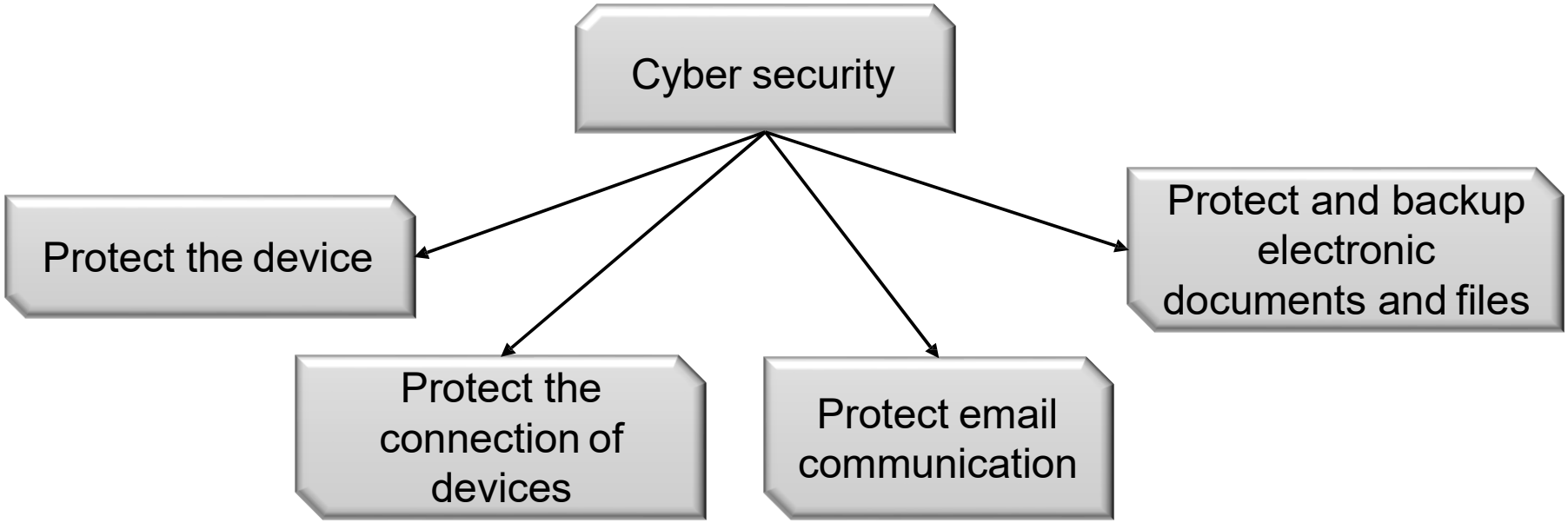
Possible Attack Strategies



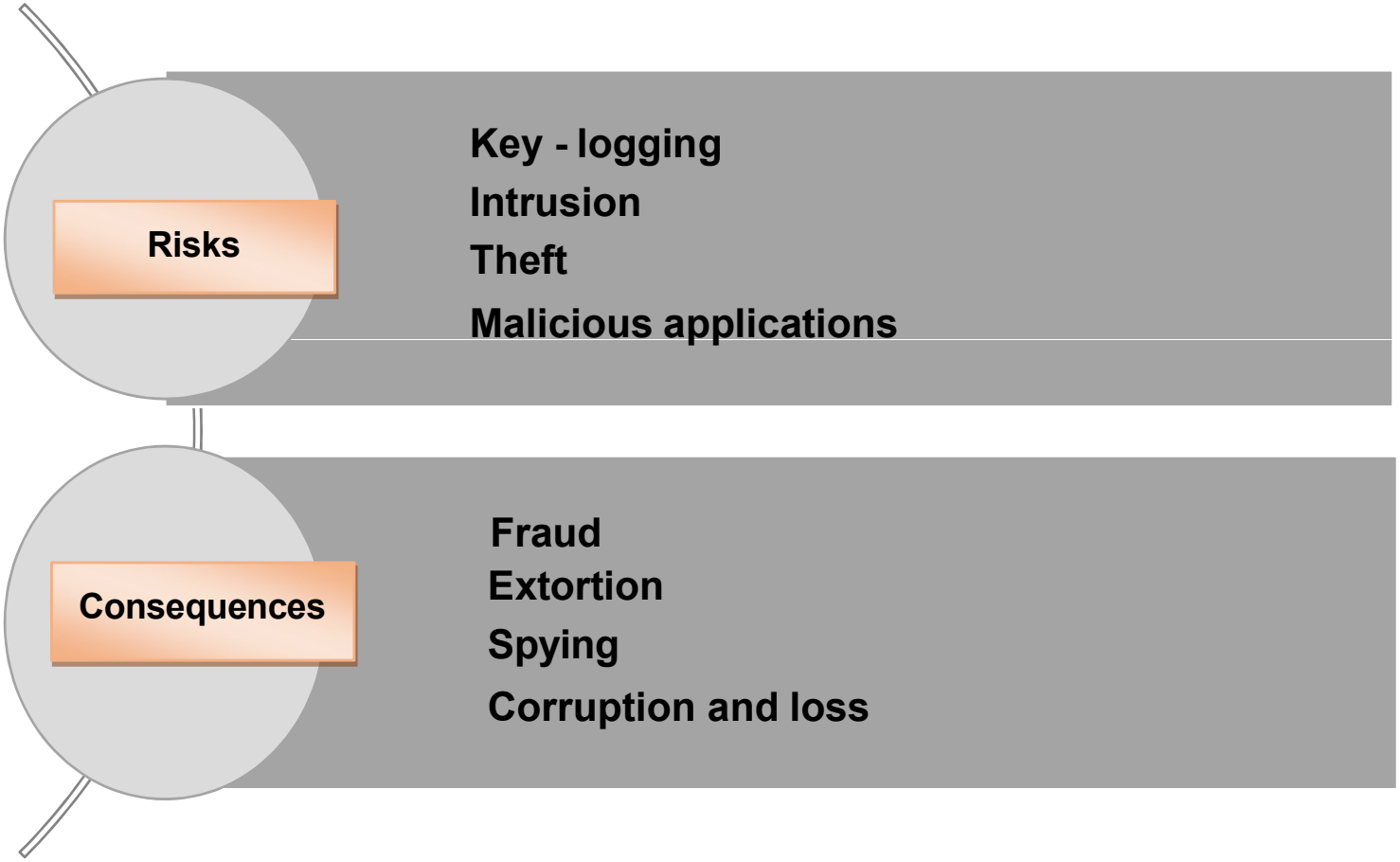
Cyber Security Core Functions



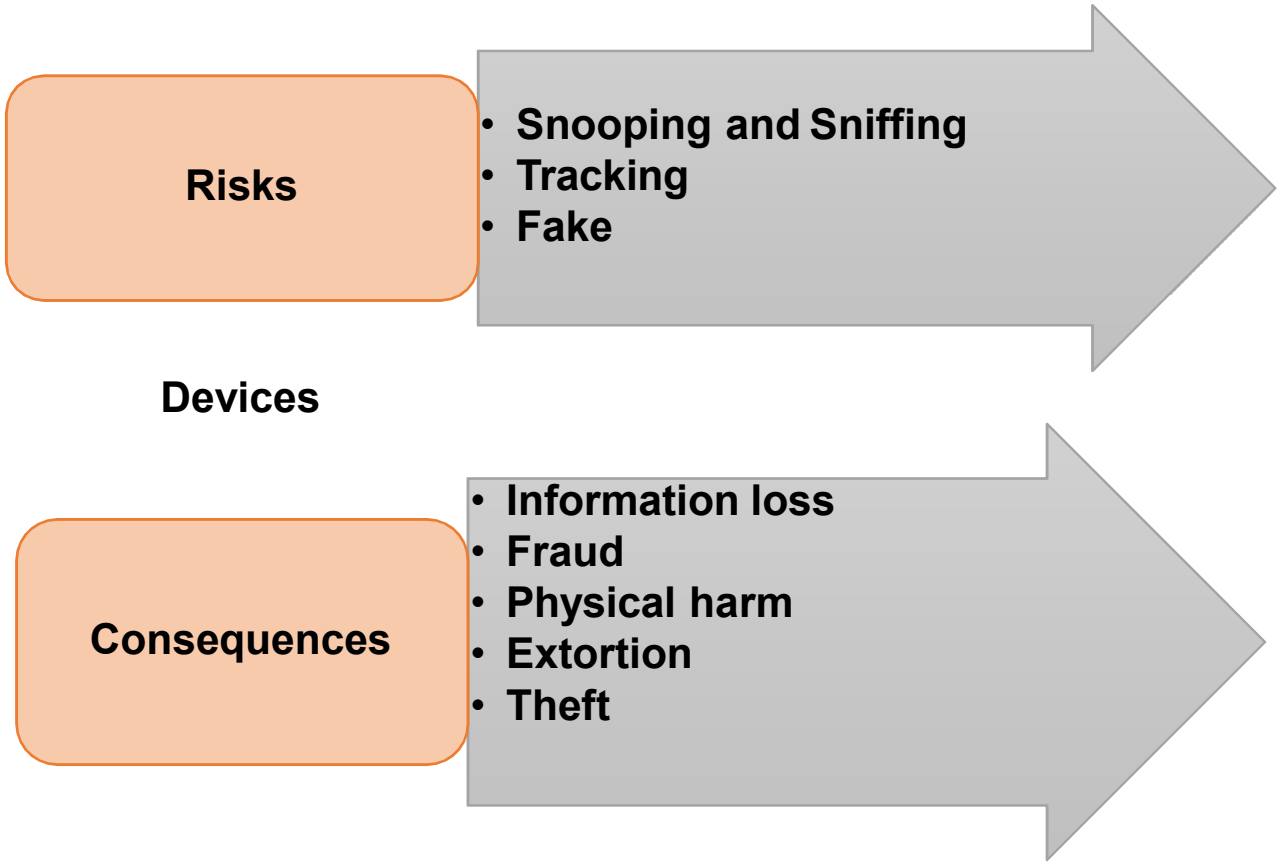
Four Important Fundamentals of Security



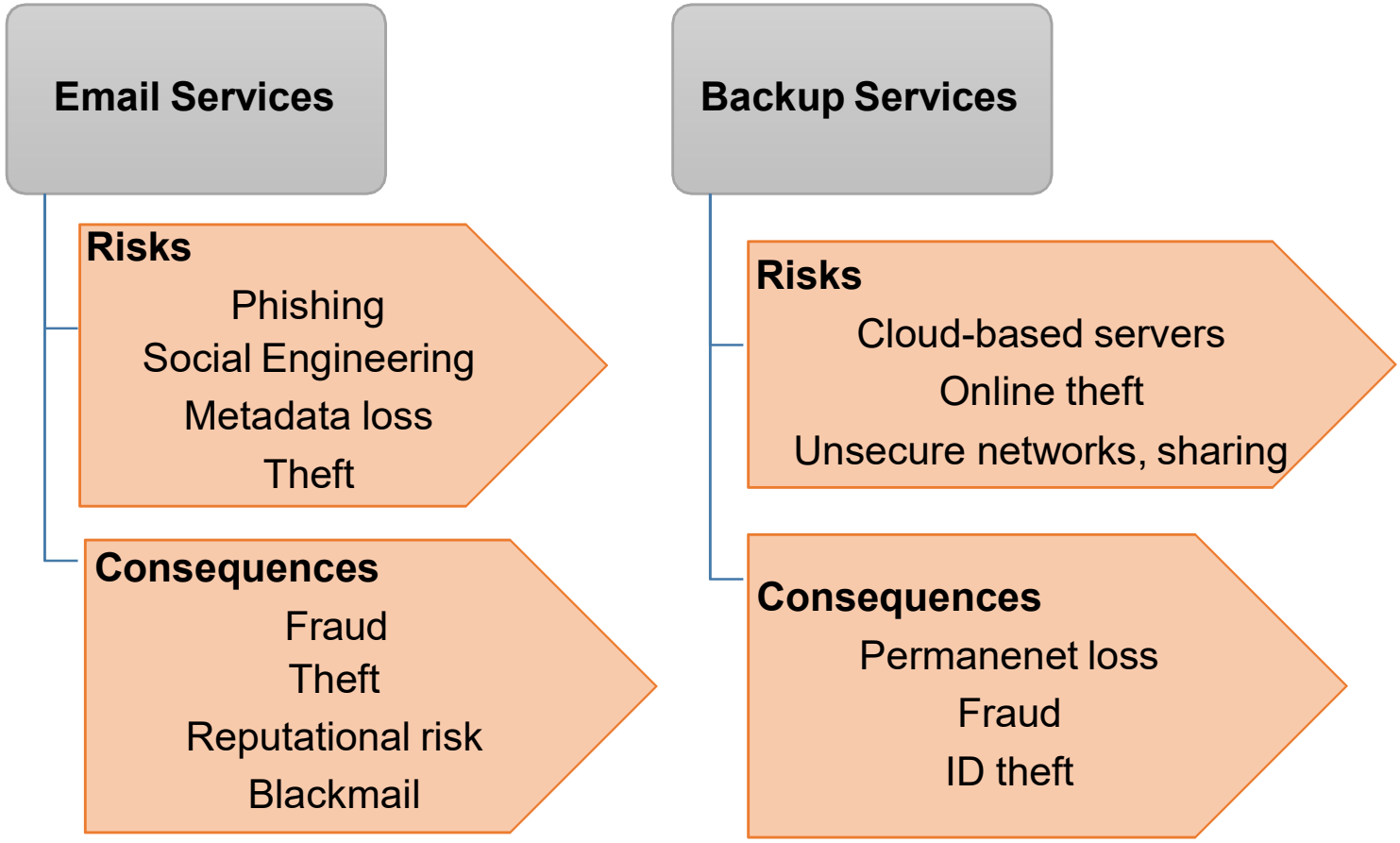
Risks and Consequences in Devices



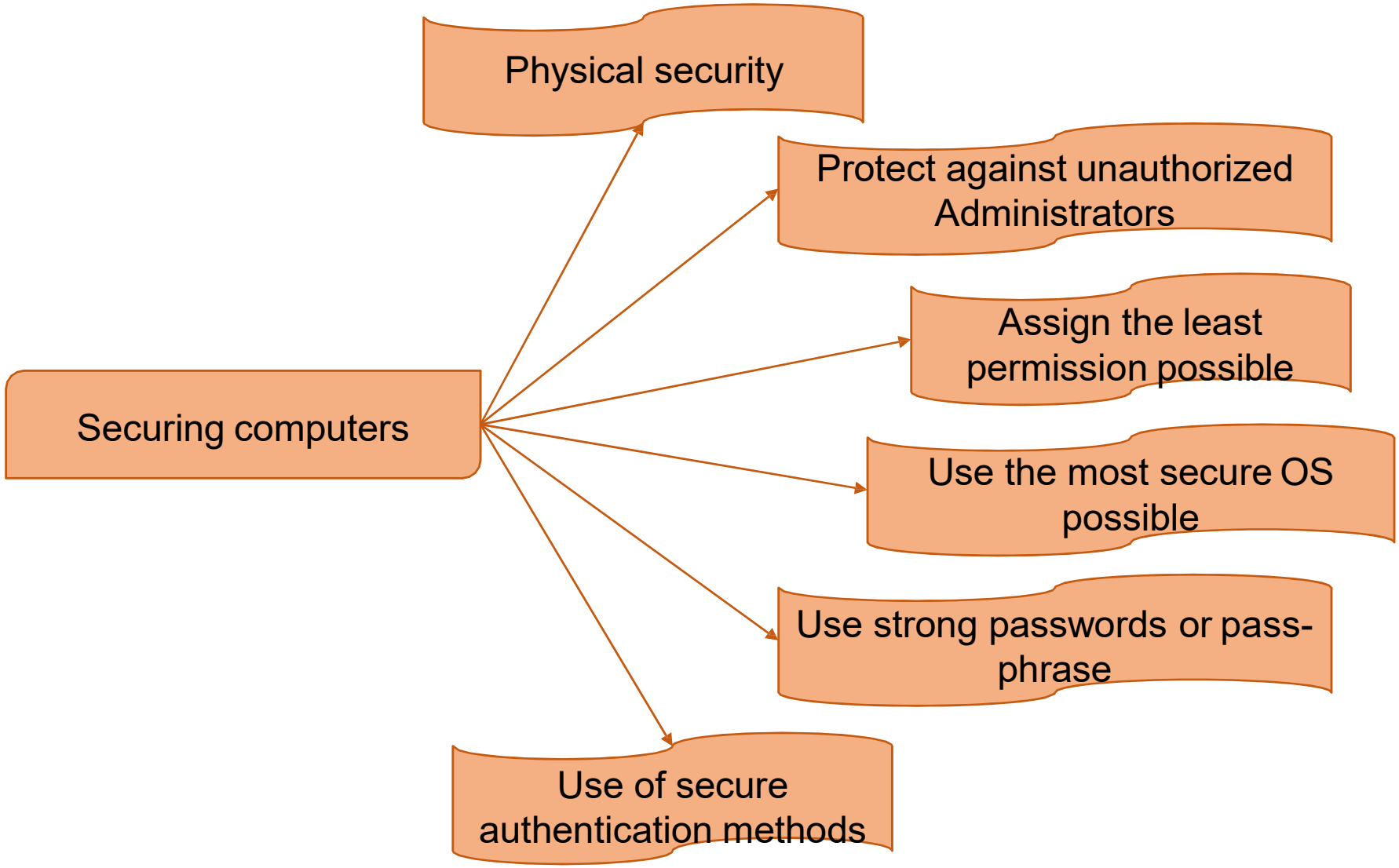
Online Communication risks and consequences



Risks and Consequences in Email and Backup Services



Other essentials in securing the Computers



Cyber Security Challenges

- Increasing number of users and adoption of technology
- Unrestricted or open access to Information
- Lack of control mechanisms
- Growing sophistication of threats
- Lack of preparedness to handle the upcoming challenges
- Inadequate and restricted handling of related crimes legally or the legal challenges

Conclusion

- Security is a very important concern today due to digitization and Information exchange
- The essentials in Cyber Security are discussed in this section
- One has to understand the challenges and the best practices to be followed to ensure security

Thank you