Introduction to Network Security

By Dr. Md. Nadir Bin Ali

Lecture-3 Outline

1.0 Introduction

1.1 Securing Networks

1.2 Network Threats

1.3 Mitigating Threats

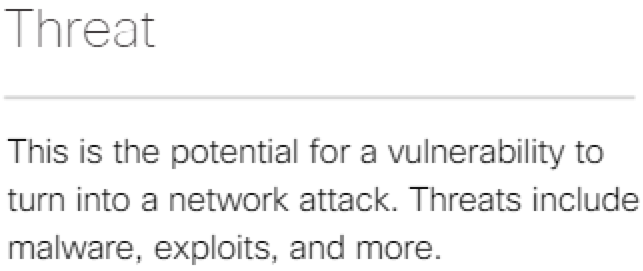
1.4 Summary

Reasons for Network Security

- Network security relates **directly to an organization's business continuity**.
- Network **security breaches** can **disrupt e-commerce, cause the loss of business data, threaten people’s privacy**, and **compromise the integrity of information.**
- These **breaches can result** in **lost revenue for corporations**, theft of intellectual property, lawsuits, and can even threaten public safety.

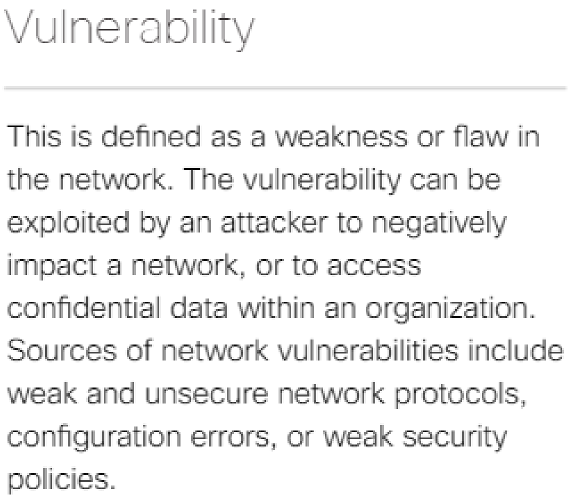
Common Network Security Terms

- Threat
- Vulnerability
- Risk
- Mitigation



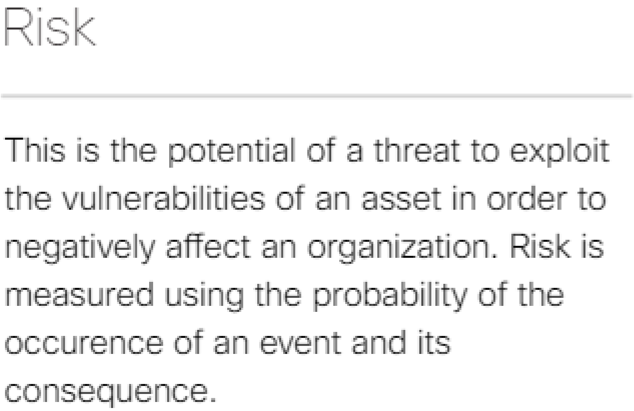
Threat

This is the potential for a vulnerability to turn into a network attack. Threats include malware, exploits, and more.



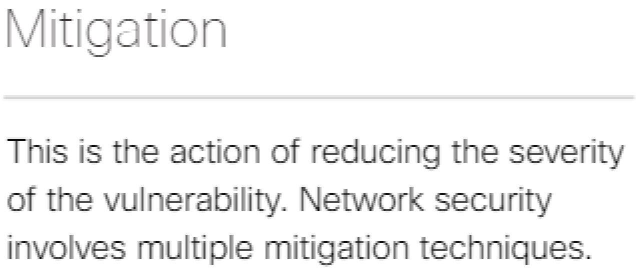
Vulnerability

This is defined as a weakness or flaw in the network. The vulnerability can be exploited by an attacker to negatively impact a network, or to access confidential data within an organization. Sources of network vulnerabilities include weak and unsecure network protocols, configuration errors, or weak security policies.



Risk

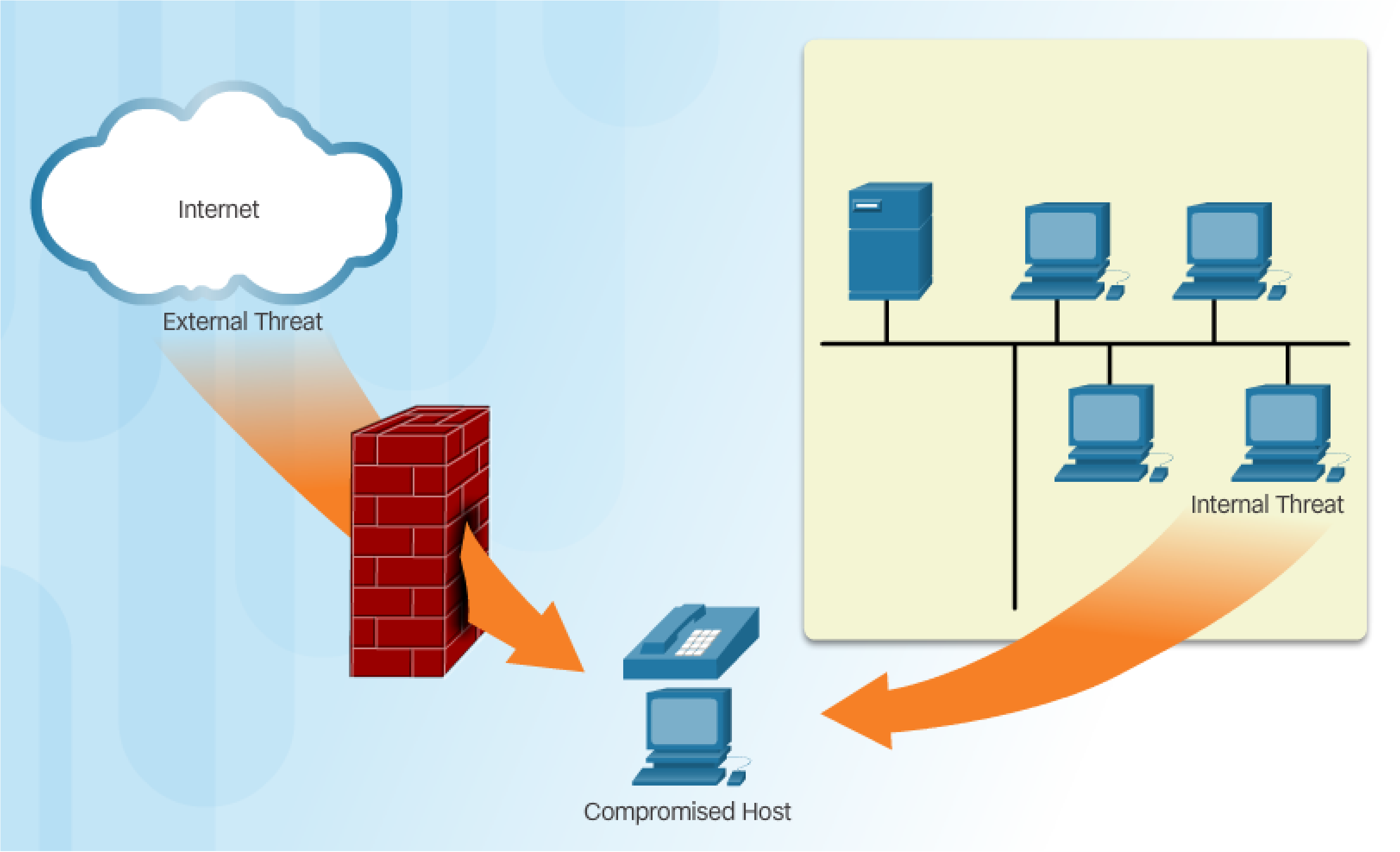
This is the potential of a threat to exploit the vulnerabilities of an asset in order to negatively affect an organization. Risk is measured using the probability of the occurence of an event and its consequence.



Mitigation

This is the action of reducing the severity of the vulnerability. Network security involves multiple mitigation techniques.

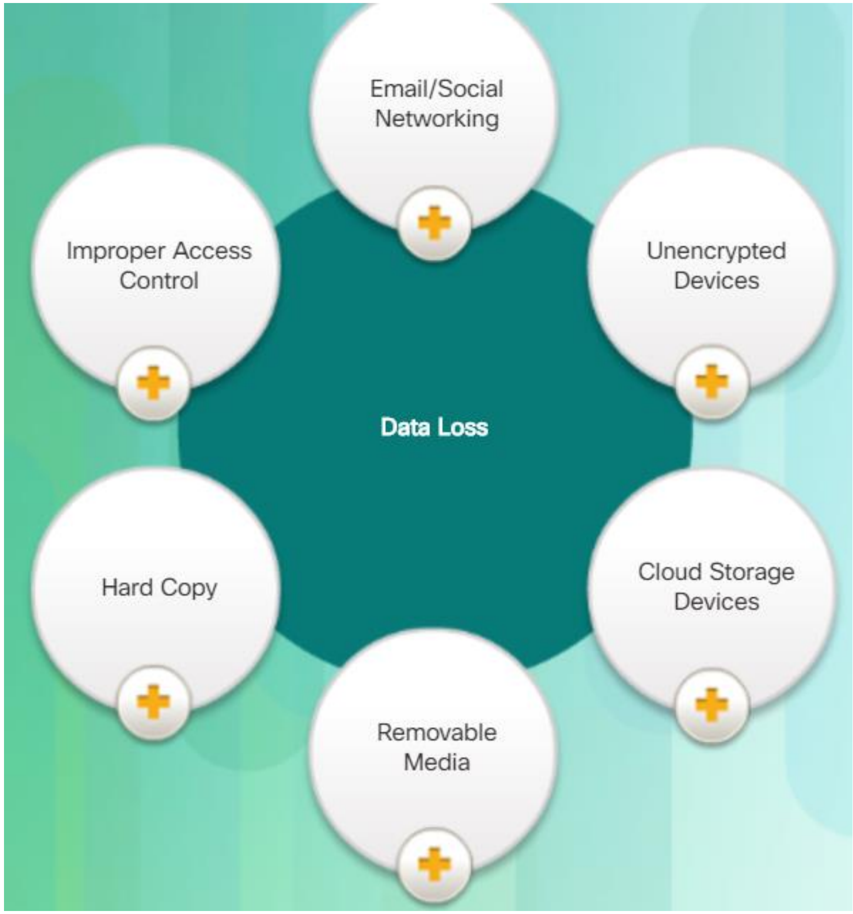
Vectors of Network Attacks



Data Loss

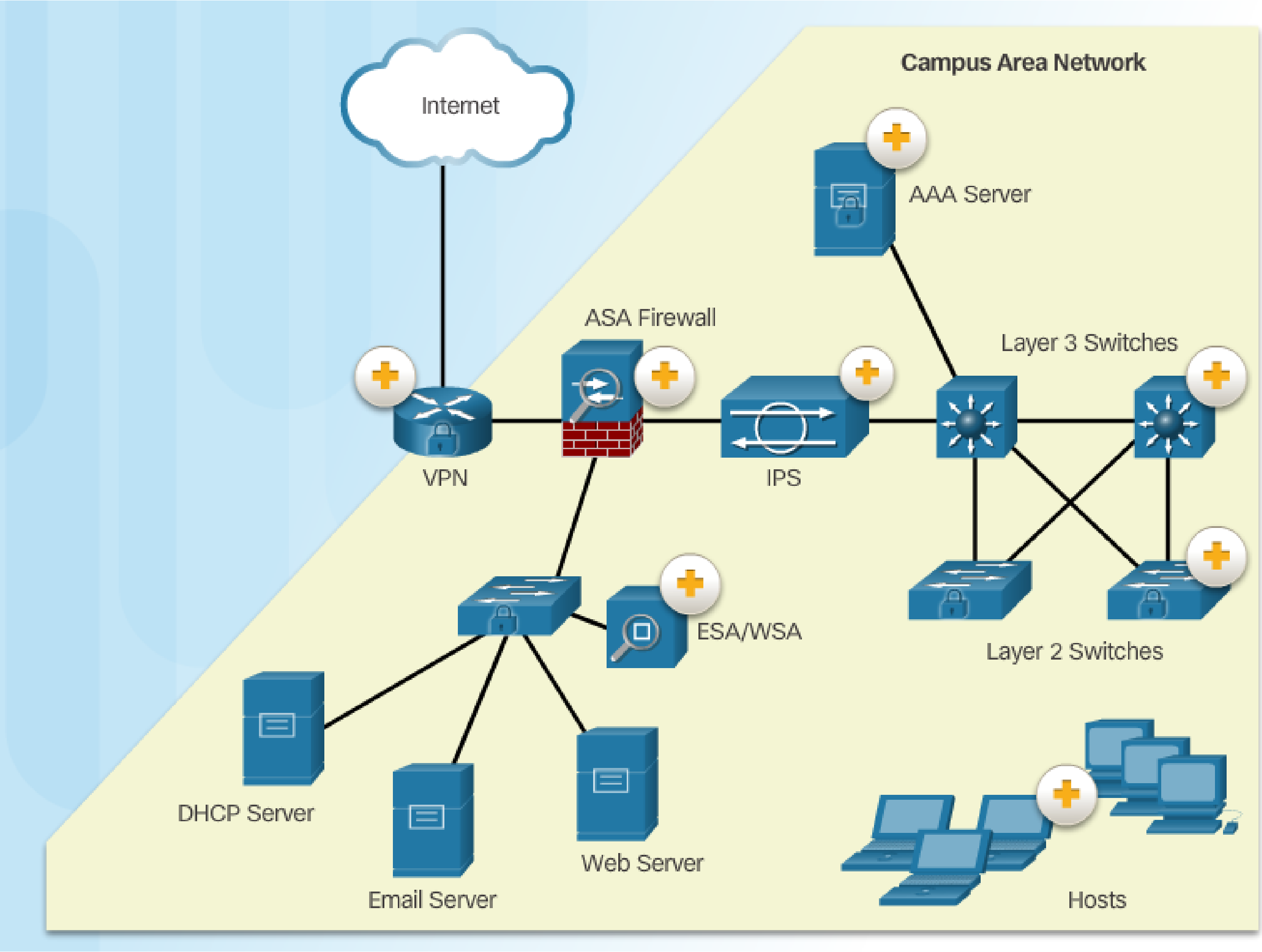
Vectors of data loss:

- Email/Social Networking
- Unencrypted Devices
- Cloud Storage Devices
- Removable Media
- Hard Copy
- Improper Access Control

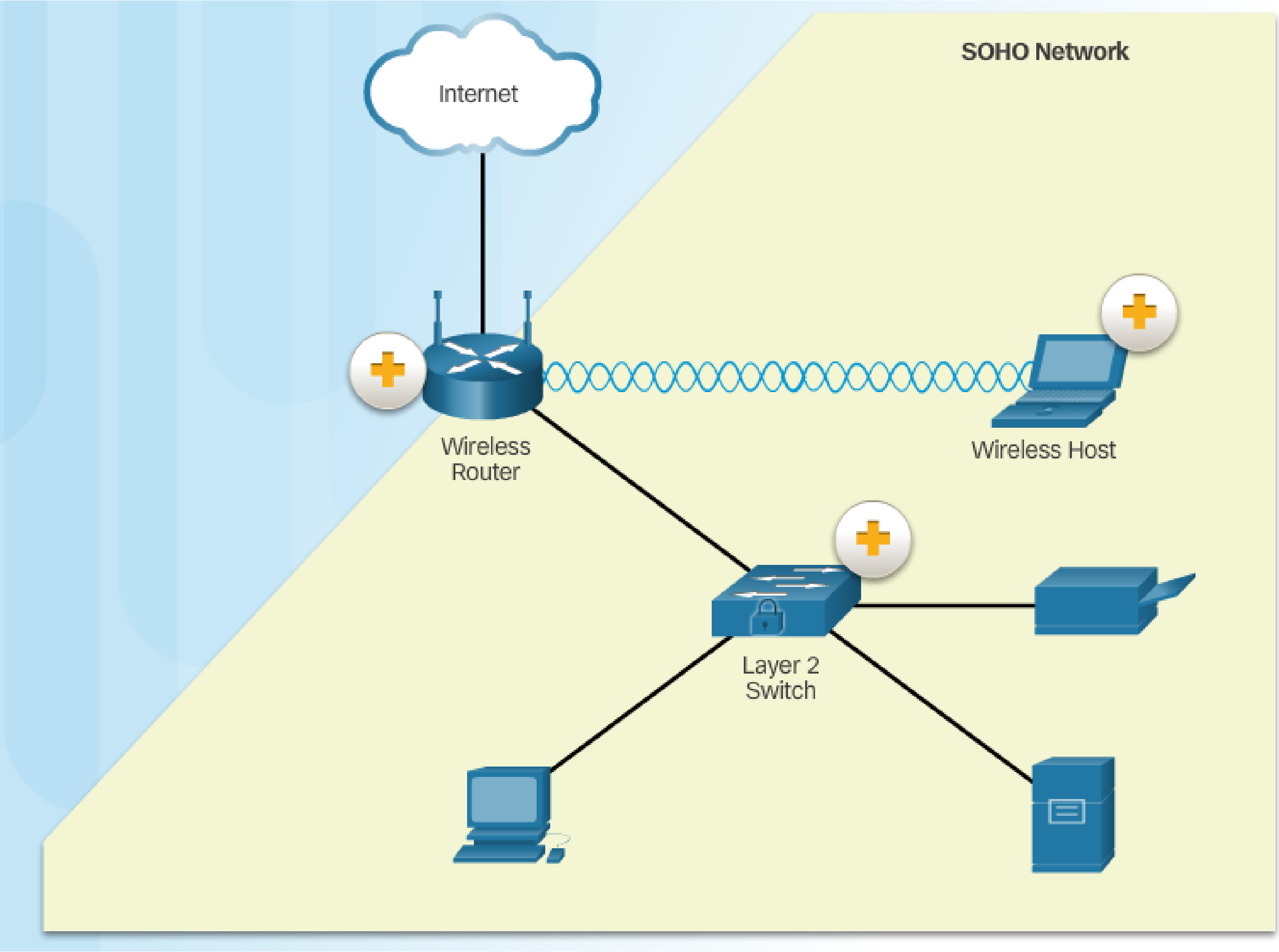


Network Topology Overview

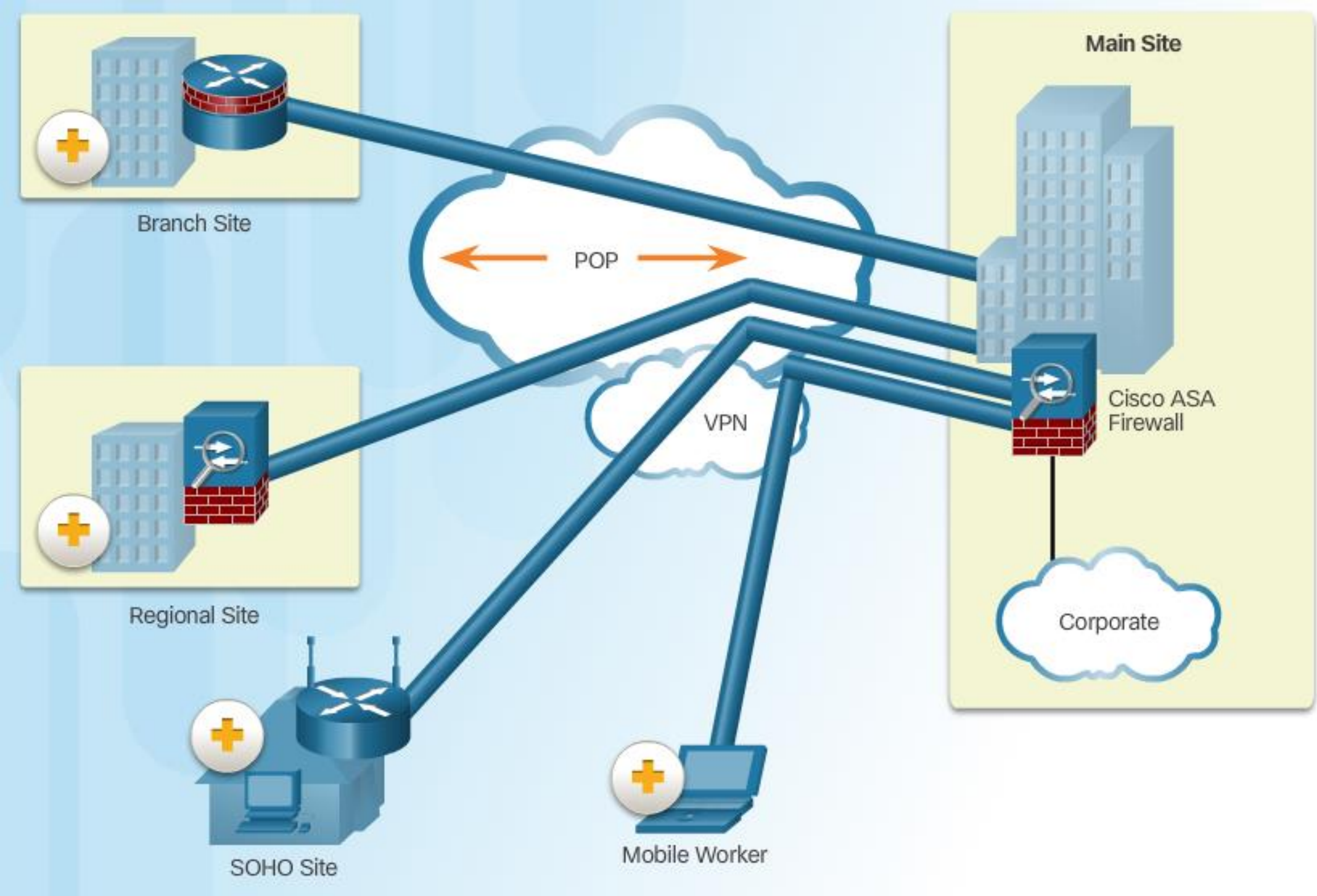
Campus Area Networks



Small Office and Home Office Networks



Wide Area Networks



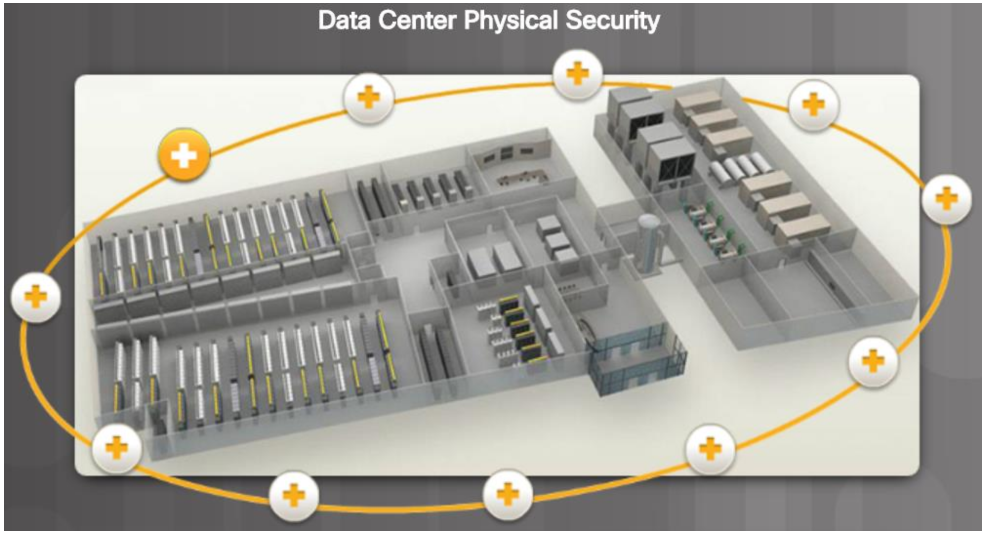
Data Center Networks

Outside perimeter security:

- On-premise security officers
- Fences and gates
- Continuous video surveillance
- Security breach alarms

Inside perimeter security:

- Electronic motion detectors
- Continuous video surveillance
- Biometric access and exit sensors



Network Threats

Upon completion of the section, you should be able to:

- Describe the evolution of network security.
- Describe the various types of attack tools used by hackers.
- Describe malware.
- Explain common network attacks.

Who is Hacking Our Networks?

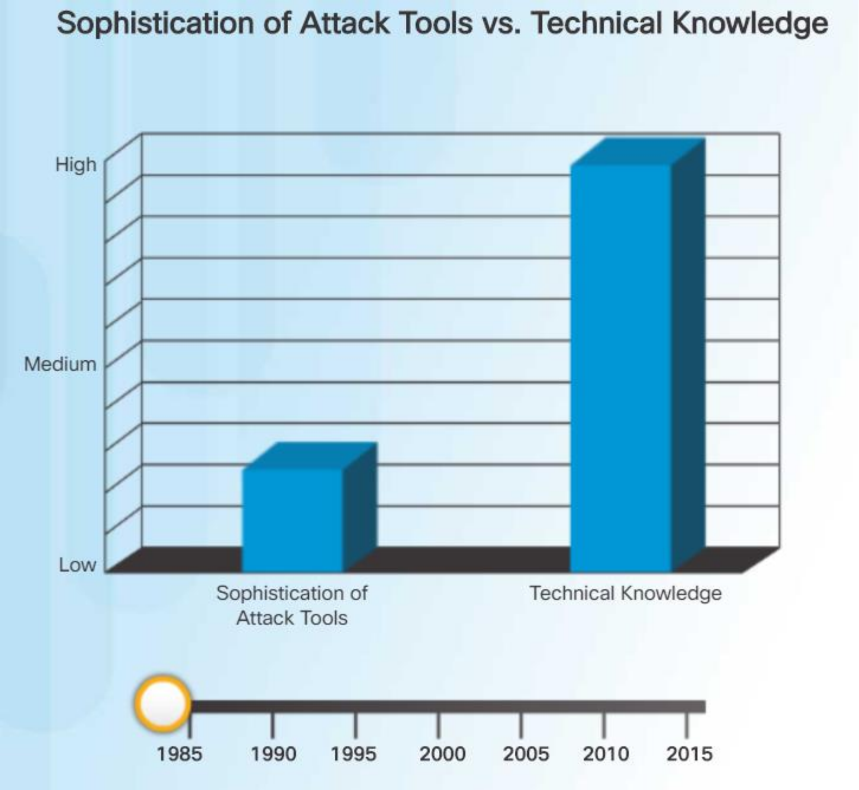
The Hacker & The Evolution of Hackers

White Hat Hackers
Grey Hat Hackers
Black Hat Hackers

Modern hacking titles:

- Script Kiddies
- Vulnerability Brokers
- Hacktivists
- Cyber Criminals
- State-Sponsored Hackers

Hacker Tools



Evolution of Security Tools

Penetration testing tools:

- Password crackers
- Wireless hacking
- Network scanning and hacking
- Packet crafting
- Packet sniffers
- Rootkit detectors
- Forensic
- Debuggers
- Hacking operating systems
- Encryption
- Vulnerability exploitation
- Vulnerability Scanners

Categories of Attack Tools

Network hacking attacks:

- Eavesdropping
- Data modification
- IP address spoofing
- Password-based
- Denial-of-service
- Man-in-the-middle
- Compromised-key
- Sniffer

Thanks for today