Current State of Cybersecurity

3.1.1

Current State of Affairs

Cyber criminals now have the expertise and tools necessary to take down critical infrastructure and systems. Their tools and techniques continue to evolve.

Cyber criminals are taking malware to unprecedented levels of sophistication and impact. They are becoming more adept at using stealth and evasion techniques to hide their activity. Lastly, cyber criminals are exploiting undefended gaps in security.

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.

Maintaining a secure network ensures the safety of network users and protects commercial interests. Organizations need individuals who can recognize the speed and scale at which adversaries are amassing and refining their cyber weaponry. All users should be aware of security terms in the table.

Security Terms	Description
Assets	An asset is anything of value to the organization. It includes people, equipment, resources, and data.
Vulnerability	A vulnerability is a weakness in a system, or its design, that could be exploited by a threat.
Threat	A threat is a potential danger to a company's assets, data, or network functionality.
Exploit	An exploit is a mechanism that takes advantage of a vulnerability.
Mitigation	Mitigation is the counter-measure that reduces the likelihood or severity of a potential threat or risk. Network security involves multiple mitigation techniques.
Risk	Risk is the likelihood of a threat to exploit the vulnerability of an asset, with the aim of negatively affecting an organization. Risk is measured using the probability of the occurrence of an event and its consequences.

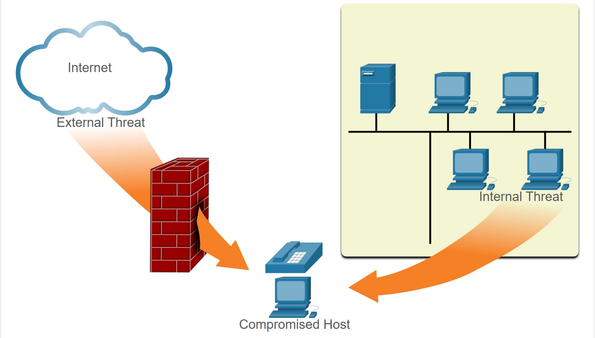
Assets must be identified and protected. Vulnerabilities must be addressed before they become a threat and are exploited. Mitigation techniques are required before, during, and after an attack.

3.1.2

Vectors of Network Attacks

An attack vector is a path by which a threat actor can gain access to a server, host, or network. Attack vectors originate from inside or outside the corporate network, as shown in the figure. For example, threat actors may target a network through the Internet, to disrupt network operations and create a denial of service (DoS) attack.

External and Internal Threats



Note: A DoS attack occurs when a network device or application is incapacitated and no longer capable of supporting requests from legitimate users.

An internal user, such as an employee, can accidentally or intentionally:

- Steal and copy confidential data to removable media, email, messaging software, and other media.
- Compromise internal servers or network infrastructure devices.
- Disconnect a critical network connection and cause a network outage.
- Connect an infected USB drive into a corporate computer system.

Internal threats have the potential to cause greater damage than external threats because internal users have direct access to the building and its infrastructure devices. Employees may also have knowledge of the corporate network, its resources, and its confidential data.

Network security professionals must implement tools and apply techniques for mitigating both external and internal threats.

3.1.3

Data Loss

Data is likely to be an organization's most valuable asset. Organizational data can include research and development data, sales data, financial data, human resource and legal data, employee data, contractor data, and customer data.

Data loss or data exfiltration is when data is intentionally or unintentionally lost, stolen, or leaked to the outside world. The data loss can result in:

- Brand damage and loss of reputation
- Loss of competitive advantage
- Loss of customers
- Loss of revenue
- Litigation/legal action resulting in fines and civil penalties
- Significant cost and effort to notify affected parties and recover from the breach

Common data loss vectors are displayed in the table.

Data Loss Vectors	Description
Email/Social Networking	Intercepted email or IM messages could be captured and reveal confidential information.
Unencrypted Devices	If the data is not stored using an encryption algorithm, then the thief can retrieve valuable confidential data.
Cloud Storage Devices	Sensitive data can be lost if access to the cloud is compromised due to weak security settings.
Removable Media	One risk is that an employee could perform an unauthorized transfer of data to a USB drive. Another risk is that a USB drive containing valuable corporate data could be lost.
Hard Copy	Confidential data should be shredded when no longer required.
Improper Access Control	Passwords or weak passwords which have been compromised can provide a threat actor with easy access to corporate data.

Network security professionals must protect the organization's data. Various Data Loss Prevention (DLP) controls must be implemented which combine strategic, operational and tactical measures.

3.1.4

Check Your Understanding - Current State of Cybersecurity

Check your understanding of the current state of cybersecurity by choosing the BEST answer to the following questions.

1. Which security term is used to describe anything of value to the organization? It includes people, equipment, resources, and data.

   - ○ Vulnerability
   - ○ Exploit
   - ◉ Asset
   - ○ Risk

2. Which security term is used to describe a weakness in a system, or its design, that could be exploited by a threat?

   - ◉ Vulnerability
   - ○ Asset
   - ○ Risk
   - ○ Mitigation

3. Which security term is used to describe a potential danger to a company's assets, data, or network functionality?

   - ○ Vulnerability
   - ○ Exploit
   - ◉ Threat
   - ○ Risk

4. Which security term is used to describe a mechanism that takes advantage of a vulnerability?

   - ◉ Exploit
   - ○ Threat
   - ○ Risk
   - ○ Mitigation

5. Which security term is used to describe the counter-measure for a potential threat or risk?

   - ○ Vulnerability
   - ○ Exploit
   - ○ Asset
   - ◉ Mitigation

6. Which security term is used to describe the likelihood of a threat to exploit the vulnerability of an asset, with the aim of negatively affecting an organization?

   - ○ Vulnerability
   - ○ Exploit
   - ○ Threat
   - ◉ Risk

Check

Show Me

Reset