B.Tech, 6^{th} Sem., Computer Networking: Security(CLASS NOTE)

Dr. Laxmidhar Biswal

April 10, 2025

Compare and contrast various types of security controls

Dr. Laxmidhar Biswal

1 Chapter 05
- Introduction
- Threat Actors
- Attributes of Actors
- Motivations

Introduction/Motivation

Compare and contrast common threat actors and motivations

Dr. Laxmidhar Biswal

Objectives of this chapter

To understand different types of cybercriminals and threat actors, their motives, and how to identify and defend against them to protect an organization.

This section discusses various types of threat actors—individuals or entities that can pose security risks. The seven major categories are:

1. Nation state
2. Advanced Persistent Threat (APT)
3. Unskilled attacker
4. Hacktivists
5. Insider threats
6. Organized crime
7. Shadow IT

Compare and contrast common threat actors and motivations

Dr. Laxmidhar Biswal

Nation state

- Cyber attackers backed by governments to pursue national interests.
- Resources & Capabilities:
  1. Have advanced tools, expert teams, and large budgets.
  2. Capable of launching highly sophisticated cyber operations.
- Types of Attacks:
  1. Espionage
  2. Data theft
  3. Infrastructure sabotage
- Motivations:
  1. Political influence
  2. Strategic advantage
  3. Election interference
  4. Cyber warfare preparation

Compare and contrast common threat actors and motivations

Dr. Laxmidhar Biswal

Nation state

- Impact:
  1. Poses threats to national security, economies, and democratic systems
  2. Often global and long-term

Compare and contrast common threat actors and motivations

Dr. Laxmidhar Biswal

Advanced Persistent Threat (APT)

- A long-term, targeted cyberattack by skilled and well-funded attackers.
- Attackers:
  - Nation-state actors
  - Cybercriminal groups
- Key characteristic:
  - Stealthy
  - Persistent
  - Data theft or slow damage
- Objective: Gain and maintain hidden access to critical systems.
- Impact: High risk to governments, corporations, and infrastructure.

Compare and contrast common threat actors and motivations

Dr. Laxmidhar Biswal

Unskilled attacker

- Individuals with limited technical skills, often using pre-made tools.
- Tools Used:
  - Off-the-shelf software
  - Tools bought from the dark web
- Example:
  - Script kiddies
  - Amateur hackers
- Capabilities: Less sophisticated than nation-states. Still able to cause disruption or data breaches
- Motivation: Personal gain, Notoriety or thrill

Compare and contrast common threat actors and motivations

Dr. Laxmidhar Biswal

Hacktivists

- Individuals or groups with ideological, political, or social motivations.
- Objective:
  - Promote a cause
  - Raise awareness
  - Push for change
- Objective:
  - Website defacement
  - Data leaks
  - Service disruptions (e.g., DDoS)
- Nature of Activity: 1) Acts as digital protest. 2) Uses technology to express dissent.

Compare and contrast common threat actors and motivations

Dr. Laxmidhar Biswal

Insider Threats

- Security threats that originate from within an organization.
- Actors:
  - Employees
  - Contractors
  - Business partners
- Types:
  - Unintentional: e.g., falling for phishing emails
  - Intentional: e.g., data theft for revenge or profit
- Access: Exploit legitimate access to compromise systems or data.
- Challenge: Hard to detect due to trusted positions and authorized access.

Compare and contrast common threat actors and motivations

Dr. Laxmidhar Biswal

Organized crime

- Cybercriminal enterprises focused on financial gain.
- Common Activities:
  - Ransomware attacks
  - Credit card fraud
  - Identity theft
- Structure:
  - Hierarchical
  - Clear division of roles (developers, attackers, launderers)
- Motivation: Purely monetary
- Concern: Their professional operations make them a major cybersecurity threat.

Compare and contrast common threat actors and motivations

Dr. Laxmidhar Biswal

Shadow IT

- Use of unauthorized apps, software, or devices within an organization.
- Reason for Use:
  - Employees aim to boost productivity
  - Streamline work without malicious intent
- Risks:
  - Creates security vulnerabilities
  - Lacks IT department oversight or control

Compare and contrast common threat actors and motivations

Dr. Laxmidhar Biswal

Attributes of Actors

- Threat actors are individuals or groups responsible for cyber threats.
- Understanding threat actors helps build effective defense strategies.
- Internal vs. External: Determines whether the threat comes from within or outside the organization.
- Resources/Funding: Indicates how well-equipped the actor is to carry out attacks.
- Sophistication/Capability: Reflects the actor's technical skill and tactical complexity.
- Purpose: Helps in tailoring incident response and defensive measures to the nature of the threat.

Compare and contrast common threat actors and motivations

Internal

- Origin: From within the organization.
-
  - Employees
  - Contractors
  - Business partners
- Advantages:
  - Familiarity with systems, networks, and workflows
  - Authorized access to sensitive data
- Intent:
  - Intentional (e.g., revenge, financial gain)
  - Unintentional (e.g., mistakes, phishing victims)
- Risk: Can cause serious damage due to their level of trust and access.

Compare and contrast common threat actors and motivations

Dr. Laxmidhar Biswal

External

- Origin: Operate outside the organization.
- Examples:
  1. Individual hackers
  2. Hacktivists
  3. Organized crime groups
  4. Nation-state actors
- Knowledge Gap: Lack internal access $\rightarrow$ rely on reconnaissance and social engineering.
- Common Attacks:
  - Espionage
  - Data theft
  - Financial fraud

Compare and contrast common threat actors and motivations

Dr. Laxmidhar Biswal

Motivations

Understanding the **motivations** behind cyberattacks is crucial for building **effective defense strategies**. Highlights common and widespread motivations behind cyber threats.

Data Exfiltration

- Goal: Steal sensitive data (e.g., personal, financial, intellectual property).
- Targets: Organizations, individuals.
- Use: Sold on the dark web or used for identity theft.
- Impact: Economic losses, legal issues, reputation damage.

Compare and contrast common threat actors and motivations

Dr. Laxmidhar Biswal

Espionage

- Actors: Nation-states or rival corporations.
- Objective: Gather intelligence or secrets covertly.
- Focus: Government databases, industrial secrets, military info.

Service Disruption

- Intent: Cause chaos or damage reputation.
- Targets: Critical infrastructure, public services.
- Motives: Political, ideological, or personal.

Compare and contrast common threat actors and motivations

Dr. Laxmidhar Biswal

Blackmail / Ransom

- Method: Use of ransomware or leaked personal content.
- Goal: Extort victims for financial or strategic gain.
- Example: Ransomware attacks demanding payment for data release.

Financial Gain

- Targets: Banks, e-commerce platforms, individuals.
- Examples: Credit card fraud, account breaches, cryptocurrency theft.

Compare and contrast common threat actors and motivations

Dr. Laxmidhar Biswal

Philosophical / Political Beliefs

- Actors: Hacktivists.
- Actions: Website defacement, leaks, denial-of-service attacks.
- Goal: Draw attention to causes or ideologies.

Ethics

- Motive: Improve cybersecurity.
- Method: Report vulnerabilities before malicious actors can exploit them.
- Impact: Strengthens system defenses.

Compare and contrast common threat actors and motivations

Dr. Laxmidhar Biswal

Revenge

- Perpetrators: Disgruntled employees, former insiders.
- Intent: Cause harm for perceived injustices.
- Example: Locking out staff by changing system passwords.

Disruption / Chaos

- Goal: Create confusion, instability, or public panic.
- Tactics: Mass outages, fake alerts, social engineering.

Cyber Warfare

- Actors: Nation-states.
- Purpose: Gain a strategic or tactical advantage.
- Usage: A modern weapon in global conflicts.

References

 https://www.ebooks.com/en-ag/book/210192090/comptia-security-sy0-601-certification-guide/ian-neil/

Question ??

The End