



Association for Cyber Security (ACS)

Empowering Protectors of the Cyber World


Session BY: Harmanpreet Singh
Date: 1st July 2024

Introduction of ACS





Internship Introduction



Benefits of Internship

Intern Responsibilities

Show Commitment!

Complete your assigned duties.

Participation: Workshops, events.

Deliverables: Reports, presentations.

What is Cybersecurity?

DEFINITION (*what does it even mean?!)*

(Is it same as “Ethical Hacking”?)

Types of Cyber Threats:-

- Malware (viruses, worms, Trojans, ransomware)
- Phishing attacks
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
- Man-in-the-Middle (MitM) attacks
- SQL Injection
- Zero-day exploits

What is Cybersecurity?

Common Cyber Security Measures:-

- Firewalls
- Antivirus and Anti-malware software
- Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)
- Encryption (data at rest and in transit)
- Multi-factor authentication (MFA)
- Regular software updates and patch management

HISTORICAL CONTEXT

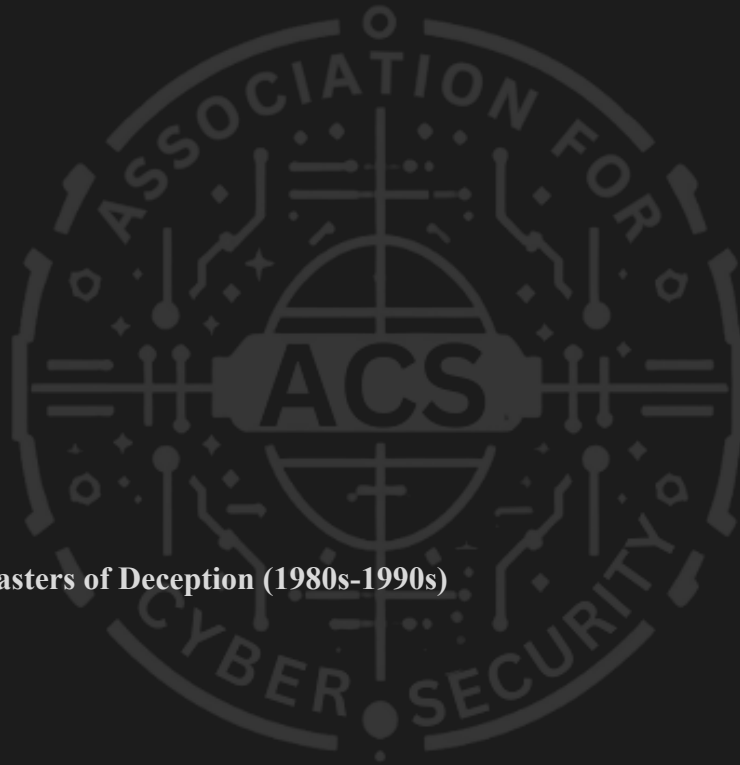
Early Cyber Threats

Initial Viruses:

- Creeper Virus (1971)
- Elk Cloner (1982)

Initial Hacks:

- Morris Worm (1988)
- Legion of Doom vs. Masters of Deception (1980s-1990s)



HISTORICAL CONTEXT

Major Incidents

Yahoo Data Breach (2013-2014)

- **Description:** Over 3 billion accounts compromised.
- **Impact:** Exposure of personal information, decreased trust, and significant financial loss.

Target Data Breach (2013)

- **Description:** 40 million credit and debit card accounts affected.
- **Impact:** Financial losses, customer trust erosion, and legal consequences.

Sony Pictures Hack (2014)

- **Description:** Release of confidential data, including employee information and unreleased films.
- **Impact:** Operational disruption, reputational damage, and significant financial cost.

WannaCry Ransomware Attack (2017)

- **Description:** Global ransomware attack affecting 230,000 computers in over 150 countries.
- **Impact:** Major operational disruptions, especially in healthcare and public services.

CIA triad

Confidentiality



Threat, Vulnerability and Risk



Types of Hackers



White Hat Hacker



Grey Hat Hacker



Black Hat Hacker

Cyber Tools and Techniques

Firewalls

Antivirus

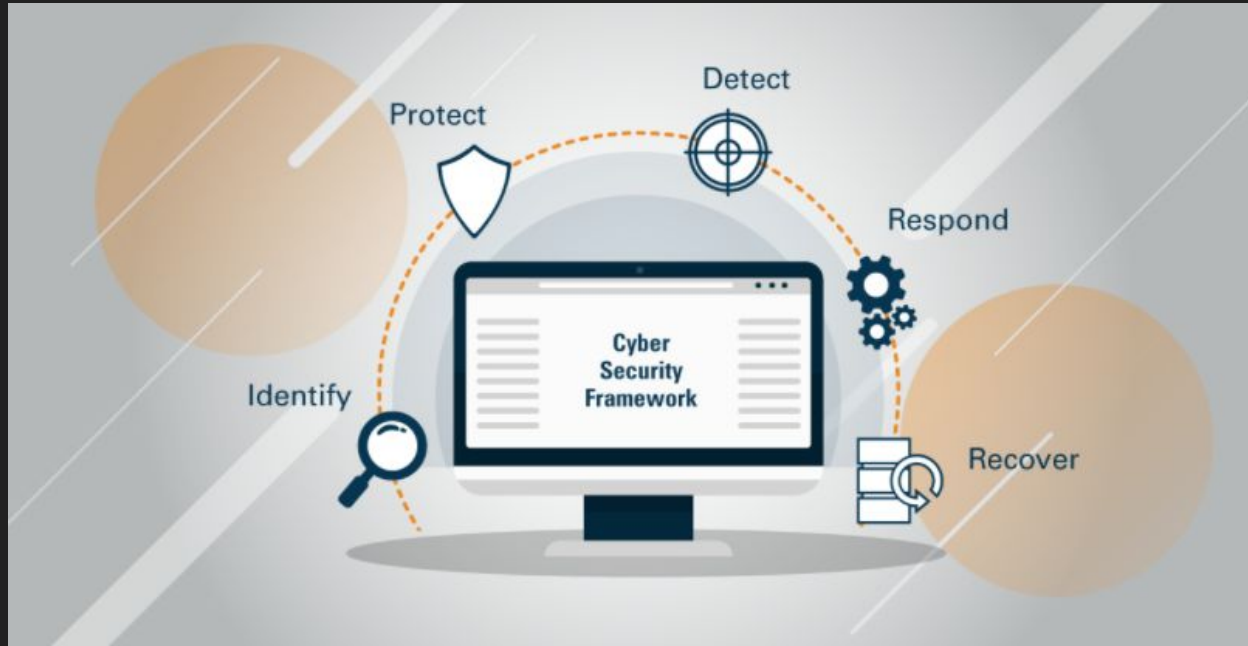
Cryptography/Encryption

IDS/IPS

Penetration Testing



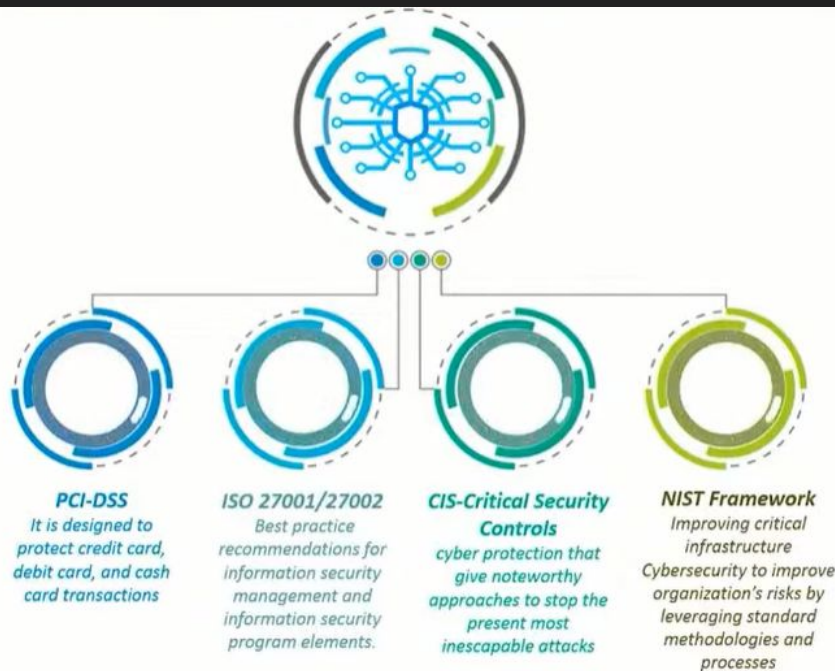
Cyber Security Frameworks



Objectives



Famous Cyber Frameworks



The Role of a CyberSec Professional

Responsibilities

- **Protect Data:**
 - **Secure Information:** Implement measures to safeguard sensitive data from unauthorized access.
 - **Example:** Use encryption, firewalls, and access controls.
- **Monitor:**
 - **Watch for Threats:** Continuously monitor systems and networks for suspicious activity.
 - **Example:** Use intrusion detection systems (IDS) and security information and event management (SIEM) tools.
- **Respond:**
 - **Handle Incidents:** Respond to and manage security incidents, mitigate damage, and restore normal operations.
 - **Example:** Incident response planning, forensics, and recovery.

The Role of a CyberSec Professional

Skills

- **Technical**
- **Problem-Solving**
- **Communication**
- **Continuous Learning**

Career Path

- **Entry-Level Roles:**
 - Security Analyst
 - IT Auditor
- **Mid-Level Roles:**
 - Security Engineer
 - Incident Responder
 - Penetration Tester
- **Advanced Roles:**
 - Security Architect
 - Cybersecurity Manager
 - Chief Information Security Officer (CISO)



Current Trends

- **Artificial Intelligence (AI) and Machine Learning (ML) in Cyber Security:**
 - **Application:** Automating threat detection and response, analyzing vast amounts of data to identify patterns and anomalies.
 - **Example:** AI-driven threat intelligence platforms that predict and neutralize potential threats.
- **Cloud Security:**
 - **Importance:** With increasing cloud adoption, securing cloud environments becomes crucial.
 - **Focus Areas:** Data protection, access management, and compliance in cloud services.
 - **Example:** Implementing cloud-specific security measures like encryption, identity and access management (IAM), and secure APIs.
- **Zero-Trust Security Model:**
 - **Concept:** Never trust, always verify. Every access request is verified, regardless of its origin.
 - **Implementation:** Micro-segmentation, continuous monitoring, and strict access controls.
 - **Example:** Multi-factor authentication (MFA) and least privilege access.

Future Directions

Emerging Threats:

- **New Risks:** Anticipating sophisticated cyber attacks such as AI-powered attacks, quantum computing threats, and advanced persistent threats (APTs).
- **Example:** AI-generated phishing emails that are more convincing and harder to detect.

Advancements in Defenses:

- **New Defenses:** Development of innovative technologies and strategies to counteract emerging threats.
- **Example:** Quantum cryptography for securing communications against quantum computing threats, advanced behavioral analytics for detecting insider threats.

A faint, circular logo is centered in the background. It features a circuit board pattern with various electronic symbols like resistors, capacitors, and integrated circuits. The words "ASSOCIATION FOR" are arched across the top, and "CYBER SECURITY" is arched across the bottom. In the center of the logo, the letters "ACSC" are visible.

Q&A Session



Thank You