GOOGLE CYBER SECURITY
Course 1: Foundations of Cyber Security

SKILLS: Cybersecurity, Security Information and Event Management (SIEM), Network Analysis, Security Controls, Security Management, Cyber Security Strategy, Incident Response, Data Ethics, Ethical Standards And Conduct, Cyber Attacks, Information Assurance, Cyber Risk

Module 1

Welcome to exciting world of Cyber

Cybersecurity, or security, is the practice of ensuring confidentiality, integrity, and availability of information by protecting networks, devices, people, and data from unauthorized access or criminal exploitation.

A threat actor is any person or group who presents a security risk.

What Is Cybersecurity?

- It's the practice of protecting **confidentiality**, **integrity**, and **availability** of data.
- It involves securing **networks, devices, people, and data** from threats or attacks.

Key Cybersecurity Terms:

Term	Simple Meaning
Compliance	Following laws and rules to avoid fines or security issues.
Security Frameworks	Guidelines or blueprints for building a secure environment.
Security Controls	Tools or actions (like firewalls, policies) to reduce risks.
Security Posture	How strong your overall cybersecurity is and how well you respond to threats.
Threat Actor	Anyone (person or group) trying to cause harm to systems or data.
Internal Threat	A security risk from someone inside (employee, vendor, partner) — accidental or intentional.
Network Security	Protecting an organization's internal network (devices, systems, data).
Cloud Security	Protecting data and apps stored on cloud servers (remote data centers).
Programming	Writing code to automate tasks, detect threats, or secure systems.

Key Takeaways:

- Knowing these terms helps you become a better **security analyst**.
- Helps in **detecting, preventing, and responding** to cyber threats.
- Stay updated using trusted glossaries like the **NIST glossary**.

Transferable Skills (soft skills from other areas)

Skill	Why It's Important in Cybersecurity
Communication	Explaining technical issues clearly to both tech and non-tech people
Problem-solving	Finding smart, quick solutions to threats and vulnerabilities
Time management	Prioritizing urgent tasks during security incidents
Growth mindset	Always learning — because tech and threats constantly evolve
Diverse perspectives	Respecting different viewpoints to solve problems more effectively

Technical Skills (hard skills specific to cybersecurity)

Skill	What It Helps With
Programming	Automating tasks like data searching and log analysis
SIEM tools	Collecting and analyzing logs to detect suspicious activity
IDS (Intrusion Detection)	Monitoring systems for unauthorized access or malware activity
Threat landscape knowledge	Understanding current hacker tactics and malware trends
Incident response	Following proper steps during and after a security breach

Core Cybersecurity Terms:

- **Cybersecurity (or security):**
  Protecting confidentiality, integrity, and availability of data, networks, devices, and people from unauthorized access or threats.
- **Cloud security:**
  Securing data and systems stored in cloud environments by configuring access for authorized users only.
- **Internal threat:**
  Security risk from a current/former employee, vendor, or partner—whether intentional or accidental.
- **Network security:**
  Protecting an organization's network infrastructure (devices, systems, data) from unauthorized access.
- **Personally Identifiable Information (PII):**
  Any data that can be used to identify a person (e.g., name, ID number, email).
- **Sensitive PII (SPII):**
  A more protected type of PII—like medical records or bank account numbers—that requires stricter handling.

- **Security posture:**
  How well an organization can protect itself and adapt to cybersecurity threats.

Module 2

Evolution of Cybersecurity

Love Letter Attack

What Was the Love Letter Attack?

- **Name**: ILOVEYOU virus (also called "Love Bug")
- **Date**: May 2000
- **Type**: Worm (self-replicating malware)
- **Attack Vector**: Social engineering via email
- **Subject Line**: ILOVEYOU
- **Attachment**: LOVE-LETTER-FOR-YOU.txt.vbs

How It Worked:

1. **Email bait**: Victims received an email with the subject **"ILOVEYOU"**, which intrigued many people.
2. **Deceptive file**: The attachment appeared to be a harmless text file, but was actually a **Visual Basic Script (.vbs)** containing malicious code.
3. **Execution**: When the victim opened the file, the worm:
   - Overwrote files (images, music, docs)
   - Sent copies of itself to all contacts in the victim's Microsoft Outlook address book
   - Spread rapidly around the world

Impact:

- **Over 10 million computers infected globally**
- **Estimated damage**: $5.5 to $8.7 billion
- Forced governments and corporations to shut down email systems temporarily

Key Lesson:

The ILOVEYOU virus showed how **human curiosity and trust can be exploited**, making **social engineering one of the most dangerous tools** in cyberattacks—even more than technical exploits.

Equifax Breach

he **Equifax breach** was a massive cybersecurity incident in **2017** that exposed the personal data of **147 million people**, making it one of the worst data breaches in U.S. history.

What Happened?

- **Date**: Discovered in **July 2017** (occurred between **May–July 2017**)
- **Company**: Equifax – a major U.S. credit reporting agency
- **Cause**: A **known vulnerability** in Apache Struts (CVE-2017-5638) was **not patched**
- **Exploit**: Hackers used the unpatched vulnerability to gain access to Equifax's systems

What Was Exposed?

- Names
- Social Security Numbers (SSNs)
- Birth dates
- Addresses
- Driver's license numbers
- Credit card information (for ~200,000 people)

Why It Was Serious

- Affected nearly **half the U.S. population**
- Involved **highly sensitive PII (Personally Identifiable Information)**
- Could lead to **identity theft, fraud**, and long-term personal and financial risks

Consequences

- **$700 million** settlement (with the FTC, CFPB, and states)
- Major **reputational damage** to Equifax
- Sparked global **calls for stronger data privacy laws**
- Led to increased awareness around **patch management and incident response**

Lessons Learned

- **Always patch known vulnerabilities promptly**
- **Encrypt sensitive data** and monitor systems
- Implement strong **incident response plans**
- Prioritize **transparency and communication** during a breach\

Brain Virus (1986)

- **What was it?**
  The **first PC virus**, created by two Pakistani brothers, **Basit and Amjad Farooq Alvi**.
- **How it worked:**
  It infected the **boot sector** of MS-DOS computers through floppy disks. When the computer started, the virus loaded into memory and could spread to other disks inserted into the drive.
- **Purpose:**
  The creators claimed it was not meant to harm but to **prevent software piracy** of their medical software.
- **Impact:**
  It unintentionally spread globally, showing how fast malware could propagate—even without the internet.

Morris Worm (1988)

- **What was it?**
  The **first worm** to spread extensively over the **early internet (ARPANET)**, created by **Robert Tappan Morris**, a student at Cornell.
- **How it worked:**
  It exploited **vulnerabilities in UNIX systems**, such as:
  - **Sendmail** (email service flaw)
  - **Finger daemon**
  - **Weak passwords**
- **Purpose:**
  Morris claimed it was meant to **measure the size of the internet**, not cause harm.
- **Impact:**
  It **slowed down thousands of systems**, causing major disruption. Estimated cost of damages: **$100,000 to $10 million**.
- **Aftermath:**
  - Morris was the **first person convicted under the U.S. Computer Fraud and Abuse Act**.
  - Led to the creation of the **first CSIRT (Computer Security Incident Response Team)**.

Common attacks and their effectiveness

Previously, you learned about past and present attacks that helped shape the cybersecurity industry. These included the **LoveLetter attack**, also called the **ILOVEYOU virus**, and the **Morris worm**. One outcome was the establishment of response teams, which are now commonly referred to as **computer security incident response teams (CSIRTs)**. In this reading, you will learn more about common methods of attack. Becoming familiar with different attack methods, and the evolving tactics and techniques threat actors use, will help you better protect organizations and people.

Phishing

Phishing is the use of digital communications to trick people into revealing sensitive data or deploying malicious software.

Some of the most common types of phishing attacks today include:

- **Business Email Compromise (BEC)**: A threat actor sends an email message that seems to be from a known source to make a seemingly legitimate request for information, in order to obtain a financial advantage.
- **Spear phishing**: A malicious email attack that targets a specific user or group of users. The email seems to originate from a trusted source.
- **Whaling**: A form of spear phishing. Threat actors target company executives to gain access to sensitive data.
- **Vishing**: The exploitation of electronic voice communication to obtain sensitive information or to impersonate a known source.
- **Smishing**: The use of text messages to trick users, in order to obtain sensitive information or to impersonate a known source.

Malware

Malware is software designed to harm devices or networks. There are many types of malware. The primary purpose of malware is to obtain money, or in some cases, an intelligence advantage that can be used against a person, an organization, or a territory.

Some of the most common types of malware attacks today include:

- **Viruses**: Malicious code written to interfere with computer operations and cause damage to data and software. A virus needs to be initiated by a user (i.e., a threat actor), who transmits the virus via a malicious attachment or file download. When someone opens the malicious attachment or download, the virus hides itself in other files in the now infected system. When the infected files are opened, it allows the virus to insert its own code to damage and/or destroy data in the system.
- **Worms**: Malware that can duplicate and spread itself across systems on its own. In contrast to a virus, a worm does not need to be downloaded by a user. Instead, it self-

replicates and spreads from an already infected computer to other devices on the same network.
- **Ransomware**: A malicious attack where threat actors encrypt an organization's data and demand payment to restore access.
- **Spyware**: Malware that's used to gather and sell information without consent. Spyware can be used to access devices. This allows threat actors to collect personal data, such as private emails, texts, voice and image recordings, and locations.

Social Engineering

Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. Human error is usually a result of trusting someone without question. It's the mission of a threat actor, acting as a social engineer, to create an environment of false trust and lies to exploit as many people as possible.

Some of the most common types of social engineering attacks today include:

- **Social media phishing**: A threat actor collects detailed information about their target from social media sites. Then, they initiate an attack.
- **Watering hole attack**: A threat actor attacks a website frequently visited by a specific group of users.
- **USB baiting**: A threat actor strategically leaves a malware USB stick for an employee to find and install, to unknowingly infect a network.
- **Physical social engineering**: A threat actor impersonates an employee, customer, or vendor to obtain unauthorized access to a physical location.

Social engineering principles

Social engineering is incredibly effective. This is because people are generally trusting and conditioned to respect authority. The number of social engineering attacks is increasing with every new social media application that allows public access to people's data. Although sharing personal data—such as your location or photos—can be convenient, it's also a risk.

Reasons why social engineering attacks are effective include:

- **Authority**: Threat actors impersonate individuals with power. This is because people, in general, have been conditioned to respect and follow authority figures.
- **Intimidation**: Threat actors use bullying tactics. This includes persuading and intimidating victims into doing what they're told.
- **Consensus/Social proof**: Because people sometimes do things that they believe many others are doing, threat actors use others' trust to pretend they are legitimate. For example, a threat actor might try to gain access to private data by telling an employee that other people at the company have given them access to that data in the past.
- **Scarcity**: A tactic used to imply that goods or services are in limited supply.
- **Familiarity**: Threat actors establish a fake emotional connection with users that can be exploited.

- **Trust**: Threat actors establish an emotional relationship with users that can be exploited over time. They use this relationship to develop trust and gain personal information.
- **Urgency**: A threat actor persuades others to respond quickly and without questioning.

Types of attacks and which CISSP security domain they relate to

Password Attacks

What it is: Trying to guess or crack passwords to gain access.
Examples:

- Brute Force
- Rainbow Table
  CISSP Domain: *Communication and Network Security*

Social Engineering Attacks

What it is: Tricking people into giving up private information.
Examples:

- Phishing, Smishing, Vishing
- Spear Phishing, Whaling
- Social Media Phishing, BEC
- Watering Hole, USB Baiting
- Physical Social Engineering
  CISSP Domain: *Security and Risk Management*

Physical Attacks

What it is: Attacks that target the physical hardware.
Examples:

- Malicious USB cable
- Malicious Flash Drive
- Card Cloning & Skimming
  CISSP Domain: *Asset Security*

Adversarial Artificial Intelligence

What it is: Misusing AI to launch smarter attacks.
CISSP Domains:

- *Communication and Network Security*
- *Identity and Access Management*

Supply-Chain Attack

What it is: Inserting malware or vulnerabilities in the supply process.
CISSP Domains:

- *Security and Risk Management*
- *Security Architecture and Engineering*
- *Security Operations*

Cryptographic Attacks

What it is: Breaking encryption or secure communications.
Examples:

- Birthday Attack
- Collision Attack
- Downgrade Attack
  CISSP Domain: *Communication and Network Security*

Threat Actor Types

1. Advanced Persistent Threats (APTs)

Highly skilled groups that secretly infiltrate networks and stay hidden for a long time.
Motivations:

- Sabotage of critical infrastructure (e.g., power grids)
- Theft of intellectual property (e.g., trade secrets, patents)

2. Insider Threats

Individuals within an organization who misuse their authorized access.
Motivations:

Sabotage

- Corruption
- Espionage
- Data leaks or unauthorized access

3. Hacktivists

Threat actors driven by political or social motives.
Motivations:

- Political protests

- Propaganda
- Campaigning for social change
- Gaining public attention

Hacker Categories

1. ***Authorized Hackers (Ethical Hackers)***

   - Work legally and follow a code of ethics
   - Help protect systems by finding and fixing vulnerabilities

2. ***Semi-Authorized Hackers (Researchers)***

   - Explore systems and find weaknesses
   - Do not exploit the vulnerabilities they discover

3. ***Unauthorized Hackers (Unethical Hackers)***

   - Operate illegally
   - Aim to steal and sell sensitive data for financial gain

Other Hacker Types

- **New/Unskilled Threat Actors (Script Kiddies):** Use existing tools to attack systems. Motivated by curiosity, revenge, or fun.
- **Contracted Hackers:** Work for pay. May take on both legal and illegal jobs.
- **Vigilante Hackers:** Claim to fight against unethical hackers. May act outside the law.

Key Takeaway

- **Threat actors** are defined by **intent** (harmful purpose).
- **Hackers** are defined by **technical skills** and **motivations** (ethical or unethical). Understanding both helps you better prepare and defend against cyber threats.

Module 3

Frameworks and Controls