GOOGLE CYBER SECURITY
Course 1: Play It Safe: Manage Security Risks

SKILLS: Information Systems Security, Risk Management, Security Information and Event Management (SIEM), Incident Response, Security Controls, Vulnerability Management, Auditing, Enterprise Security

Module 1

Security Domains

This module explains the focus of CISSP's eight security domains. Then, primary threats, risks, and vulnerabilities to business operations are identified and defined, along with a discussion of the threats, risks, and vulnerabilities entry-level security analysts focus on most. Additionally, NIST's Risk Management Framework (RMF) is introduced.

What you'll learn

- CISSP's eight security domains
- Security frameworks and controls
- Security audits
- Basic security tools
- Protect assets and data

Overview of the Cybersecurity Program

Purpose of the Program:
The program is designed to equip you with the **knowledge, skills, and tools** necessary to work effectively in the **world of cybersecurity** (also called **security**).

What You'll Learn:

1. **CISSP's 8 Security Domains**
   - You'll get an overview of the **eight core domains** from the **CISSP (Certified Information Systems Security Professional)** framework.
   - These domains represent the **main focus areas** in cybersecurity.
2. **Threats, Risks, and Vulnerabilities**
   - You'll dive deeper into:

    - What **threats** are (potential dangers),
    - What **risks** mean (the chances that a threat will exploit a vulnerability),
    - And what **vulnerabilities** are (weaknesses in systems or processes).
3. **Three Layers of the Web:**
    - **Surface Web** – the part of the internet we use every day.
    - **Deep Web** – data not indexed by search engines (like academic databases, private emails).
    - **Dark Web** – anonymous part of the web often associated with illegal activity.

      You'll see examples to help understand each of these.

4. **Types of Attacks:**
    - You'll be introduced to different kinds of **cyber attacks** (like phishing, malware, ransomware, etc.), which will be explained more later in the course.
5. **Risk Management with NIST RMF:**
    - You'll learn about the **NIST Risk Management Framework** – a structured approach developed by the **National Institute of Standards and Technology (NIST)**.
    - It helps **identify, assess, and manage cybersecurity risks** in organizations.

Why This Matters:

- These topics are considered **foundational** in cybersecurity.
- Gaining a strong understanding will help you:
    - **Prevent attacks**
    - **Reduce risks**
    - **Protect organizations** from daily threats

CISSP security domains:

1. Security and Risk Management

Focus Areas:

- **Defining goals & objectives**: Helps reduce risks to sensitive data like PII (Personally Identifiable Information)
- **Risk mitigation**: Having rules and processes to reduce the impact of security events (e.g., breaches)
- **Compliance**: Developing internal security policies based on laws, standards, and regulations
- **Business continuity**: Ensuring daily operations continue during disruptions using recovery plans
- **Legal and ethical behavior**: Following laws and ethical guidelines to avoid negligence, abuse, and fraud

2. Asset Security

Focus Areas:

- Protecting both **digital and physical assets**
- Ensuring proper:
  - **Storage**
  - **Maintenance**
  - **Retention**
  - **Destruction** of sensitive data (like PII or SPII – Sensitive PII)
- Tracking **who has access** to what data
- Example: Security analysts may oversee the proper destruction of hard drives to prevent data leaks

3. Security Architecture and Engineering

Focus Areas:

- Implementing secure **tools**, **systems**, and **processes** to protect data
- Promoting the idea of **shared responsibility**:
  - Everyone in the organization should actively participate in maintaining security
  - Encouraging users to report suspicious activity or concerns

4. Communication and Network Security

Focus Areas:

- Securing **physical networks**, **wireless networks**, and **cloud communications**
- Protecting remote connections, such as:
    - Insecure Bluetooth
    - Public Wi-Fi
- Example: Security teams may disable risky communication channels to reduce unsafe user behavior

5. Identity and Access Management (IAM)

Purpose:
To control **who can access what** in an organization by using **access and authorization policies**.

Key Goals:

- Ensure users only have access to what they need.
- Prevent unauthorized access.
- Reduce risk to systems and data.

Real-world example:

- If everyone uses the same admin login, you can't track individual actions. This makes it impossible to investigate who did what during a breach.

IAM Core Components:

1. **Identification** – Verifying who a user is (e.g., username, ID card, fingerprint)
2. **Authentication** – Proving identity (e.g., password, PIN)
3. **Authorization** – Granting access based on user roles
4. **Accountability** – Logging and monitoring user actions

6. Security Assessment and Testing

Purpose:
To **evaluate and improve security controls** regularly through testing, auditing, and analysis.

Key Activities:

- Conduct **security control tests**
- Perform **security audits**
- Collect and analyze **security data**

These actions help detect risks and vulnerabilities and improve the organization's defense mechanisms.

Example:
Introducing **multi-factor authentication (MFA)** after a test shows that password-only access is weak.

7. Security Operations

Purpose:
To **detect, respond to, and investigate security incidents** while also preventing future ones.

Key Steps:

1. **Incident response** – Act quickly during an active attack to reduce damage
2. **Forensic investigation** – Collect digital/physical evidence to understand the breach
3. **Post-incident improvement** – Analyze the incident to strengthen future defenses

8. Software Development Security

Purpose:
To integrate **security into every phase of the software development lifecycle (SDLC)**.

Key Practices:

- Use **secure coding guidelines**
- Perform **security reviews** during design, development, testing, and deployment
- Conduct **penetration testing** before releasing the software

Example:

- Do a secure design review early
- Review code for vulnerabilities during development
- Test for security flaws before launching the product

Conclusion:

Understanding all **eight domains** helps you see how organizations build and maintain strong security. These domains also highlight the essential work of cybersecurity teams in defending assets, systems, and data.

Let me know when you're ready to go over threats, risks, vulnerabilities, ransomware, and the layers of the web.

What Are Assets?

- An **asset** is anything valuable to an organization (digital or physical).
- Examples: Computers, office spaces, customer PII (Personally Identifiable Information), patents, and intellectual property.

1. Threats

- A **threat** is anything that can **negatively impact assets**.
- Example: **Social engineering attacks**
  - Specifically, **phishing**: Tricking users (via fake emails or links) into giving up sensitive data like usernames or banking info.

2. Risks

- A **risk** is the **potential for a threat to exploit a vulnerability** and impact an asset's:
  - **Confidentiality** (privacy)
  - **Integrity** (accuracy)
  - **Availability** (accessibility)
- Think of **risk** as the **likelihood** of something bad happening.
- **Example of a risk**: No backup plan for recovering important data in case of a breach or accident.

Risk Levels:

- **Low risk**: Public data (e.g., website content) – no serious impact if exposed.
- **Medium risk**: Sensitive internal data (e.g., unreleased earnings reports) – may hurt reputation or finances.
- **High risk**: Protected data (e.g., SPII, PII, intellectual property) – serious legal, financial, and operational consequences if compromised.

3. Vulnerabilities

- A **vulnerability** is a **weakness** that a **threat can exploit**.
- **Examples:**
  - Outdated firewalls or software
  - Weak passwords
  - Unprotected sensitive data
  - Even people (e.g., unaware employees) can be vulnerabilities
- Important note:
  Both a vulnerability and a threat must exist for a risk to occur.

Role of Entry-Level Analysts

- Educate staff to identify threats (e.g., phishing awareness)
- Use security tools (e.g., access cards to restrict building entry)
- Encourage reporting of suspicious activity
- Monitor and document access to critical assets
- Help the organization **reduce risk** by **managing vulnerabilities**

Ransomware

- **Ransomware** is a type of **malware** used by threat actors to **encrypt an organization's data**.
- Once encrypted:
  - Systems are frozen
  - Devices become unusable
  - Confidential data is locked
- The attacker demands a **ransom payment** in exchange for a **decryption key** (used to unlock the data).
- These events, including negotiations or leaked data, often happen via the **dark web** due to its secrecy.

Three Layers of the Web

1. **Surface Web**
   - Publicly accessible and searchable via standard web browsers
   - Examples: Social media, online shopping, news sites
2. **Deep Web**
   - Not indexed by search engines; requires authorization
   - Example: Company intranet (for internal use only)
3. **Dark Web**
   - Only accessible through special tools like **Tor**
   - Known for anonymous activity; often used for illegal actions like selling stolen data

Three Key Impacts of Threats, Risks, and Vulnerabilities

1. **Financial Impact**
   - High costs from:
     - Production/service interruption
     - Fixing systems
     - Fines due to **non-compliance**
   - Example: After a ransomware attack, restoring operations and paying penalties can be very expensive
2. **Identity Theft**

   - Storing sensitive information like **PII** (Personally Identifiable Information) introduces risk
   - Leaked PII can be sold on the dark web
   - Affects employees, customers, and vendors
3. **Reputational Damage**
   - Loss of customer trust and loyalty
   - Bad publicity and negative media coverage
   - Can lead to long-term harm, customer loss, and even legal penalties

NIST Risk Management Framework (RMF)

What is the NIST RMF?

- Developed by the **National Institute of Standards and Technology (NIST)**.
- A structured **7-step process** to help organizations **manage risks, threats, and vulnerabilities**.
- While entry-level analysts may not perform all steps, understanding the full process is valuable and can help you stand out during job applications.

The 7 Steps of the NIST Risk Management Framework (RMF)

1. Prepare

- **Goal:** Get ready to manage risks **before** any breach happens.
- **Tasks for analysts:** Monitor for risks, identify helpful controls, and gather information.
- **Example:** Watching for suspicious activity or known vulnerabilities.

2. Categorize

- **Goal:** Understand what's at risk and how it could impact **confidentiality, integrity, and availability (CIA)**.
- **Tasks for analysts:** Follow processes to reduce risks to critical assets, like customer data.
- **Example:** Categorizing data as low, medium, or high risk.

3. Select

- **Goal:** Choose and document security controls.
- **Tasks for analysts:** Help update security documentation like **playbooks** or **guidelines**.
- **Example:** Recording which controls are used to protect employee login data.

---

4. Implement

- **Goal:** Put the selected security controls and privacy plans into action.
- **Tasks for analysts:** Apply security changes to fix observed issues.
- **Example:** Updating password policies if users often request password resets.

5. Assess

- **Goal:** Check if controls are working correctly.
- **Tasks for analysts:** Evaluate how effective tools, procedures, and systems are.
- **Example:** Spotting weaknesses in current defenses and suggesting changes.

6. Authorize

- **Goal:** Accept accountability for risks that remain.
- **Tasks for analysts:** Create reports, write action plans, and help define project goals.
- **Example:** Documenting risk reports to present to management.

7. Monitor

- **Goal:** Continually track system performance and risk levels.
- **Tasks for analysts:** Daily monitoring, identifying any deviation from security goals.
- **Example:** If current systems aren’t keeping risk low, flag it for updates.

Key Reminder:

Even if you don’t set up these processes yourself, your job will involve **ensuring they're functioning correctly** to reduce risk for your organization and its customers.

Let me know if you'd like a simplified visual of the 7 steps or help memorizing them.

Glossary terms from module 1

Assess: The fifth step of the NIST RMF that means to determine if established controls are implemented correctly

Authorize: The sixth step of the NIST RMF that refers to being accountable for the security and privacy risks that may exist in an organization

Business continuity: An organization's ability to maintain their everyday productivity by establishing risk disaster recovery plans

Categorize: The second step of the NIST RMF that is used to develop risk management processes and tasks

External threat: Anything outside the organization that has the potential to harm organizational assets

Implement: The fourth step of the NIST RMF that means to implement security and privacy plans for an organization

Internal threat: A current or former employee, external vendor, or trusted partner who poses a security risk

Monitor: The seventh step of the NIST RMF that means be aware of how systems are operating

Prepare: The first step of the NIST RMF related to activities that are necessary to manage security and privacy risks before a breach occurs

Ransomware: A malicious attack where threat actors encrypt an organization’s data and demand payment to restore access

Risk: Anything that can impact the confidentiality, integrity, or availability of an asset

Risk mitigation: The process of having the right procedures and rules in place to quickly reduce the impact of a risk like a breach

Security posture: An organization’s ability to manage its defense of critical assets and data and react to change

Select: The third step of the NIST RMF that means to choose, customize, and capture documentation of the controls that protect an organization

Shared responsibility: The idea that all individuals within an organization take an active role in lowering risk and maintaining both physical and virtual security

Social engineering: A manipulation technique that exploits human error to gain private information, access, or valuables

Vulnerability: A weakness that can be exploited by a threat

Module 2

Security Frameworks and Controls