

Introduction to Cybersecurity

Study Guide

Core Security Concepts (main takeaway): Risk is not a score or a label. Risk is a reviewable path to a specific asset. The chapter's job is to make you able to write one disciplined chain, test it for specificity, present-tense reality, and observable outcomes, and only then use CIA as outcome vocabulary and friction as the improvement target.

What you must remember

The model

Asset → Entry Point → Weak Spot → Damage

If you can reliably produce this chain, you can do disciplined security reasoning in new systems.

What each word means

Component	Meaning
Asset	The specific system object or function that must not be harmed.
Entry Point	The typical workflow where legitimate activity begins.
Weak Spot	A present-tense condition that lowers resistance right now.
Damage	The observable outcome if the path completes (something someone would notice).

The three tests

A chain is ready for review only if it passes:

- Concrete Test: The asset is a specific thing.
- Current Test: The weak spot is a real condition that exists now.
- Witness Test: A non-technical manager could recognize the damage.

CIA, used correctly

CIA is outcome vocabulary, not an explanation.

- Confidentiality: The wrong party saw information.
- Integrity: Information or behaviour is incorrect.

- Availability: A required function fails when needed.

Rule: Apply CIA only after the damage is clear.

The friction rule

Good security makes the wrong thing expensive and the right thing cheap.

As a target: increase the cost of unauthorized use by $\sim 100\times$ while increasing authorized routine work by $<1.1\times$.

The core process to practice

Use this sequence until it becomes automatic:

1. Read for nouns and workflows. Identify candidate assets (things) and entry points (normal routines).
2. Choose one asset. Pick the thing that, if harmed, creates the problem the scenario describes.
3. Name the entry point. Describe the legitimate workflow that makes the asset reachable.
4. State the weak spot in the present tense. Describe the condition that makes misuse easier than it should be.
5. Write observable damage. Describe what would be noticed, not what could be exploited.
6. Run the Acid Test. Fix only the failing component. Repeat.
7. Classify with CIA. Pick the primary harm and justify it from the damage.
8. (Optional) Improve friction. Propose one change that raises resistance without disrupting normal work.

Common traps to watch for

- Treating the model as a template to fill in rather than a claim to make precise.
- Using vague words that hide missing thinking (“compromised,” “hacked,” “insecure,” “exposed”).
- Confusing workflow with weakness (the entry point is not the flaw).
- Writing weak spots as possibilities (“could,” “might”) instead of present conditions (“is,” “allows,” “lacks”).
- Stopping at CIA labels without damage you can point to.

Readiness questions

Answer these without looking anything up. If you cannot answer one, it tells you exactly what to practice next.

Model recall

1. Write the four-part chain from memory.
2. In one sentence each, define Asset, Entry Point, Weak Spot, and Damage.

Identification skill

3. Given a short scenario, can you name an asset as a specific system thing (not a principle or a whole system)?
4. Can you name an entry point as a normal workflow without using any attack terms?
5. Can you write a weak spot as a present-tense condition that could be checked today?
6. Can you write damage as an observable outcome that someone outside security would notice?

Acid Test discipline

7. For each Acid Test, what would a failing answer look like?
8. When a chain fails one test, can you rewrite only the failing component and leave the rest intact?

CIA correctness

9. Explain the difference between a CIA label and a full chain.
10. Given an observable damage statement, can you classify it as C, I, or A and justify it using only the damage?

Friction thinking

11. What is one example of a change that increases friction for the wrong action without adding much friction for the right action?
12. What is one example of a change that sounds like security work but does not actually change the weak spot?

Practice questions

Answer these in writing. Aim for short, precise answers. If you get stuck, that is the point: it tells you what part of the process still needs practice.

Definitions and recall

1. Write the four-part chain from memory.
2. Define Asset in one sentence. Include the word “specific.”
3. Define Entry Point in one sentence. Include the word “normal.”

4. Define Weak Spot in one sentence. Include the phrase “present-tense condition.”
5. Define Damage in one sentence. Include the word “observable.”
6. In one sentence, explain why CIA is not an explanation.

Extraction from scenarios

7. When reading a scenario, what are the two kinds of information you are hunting for first?
8. What is a sign that you have chosen an “asset” that is too broad?
9. What is a sign that your “entry point” is actually an attack description?
10. What is a sign that your “weak spot” is not a condition that exists right now?
11. What is a sign that your “damage” is still vague?

Writing a reviewable claim

12. Write a sentence template you can use to state an asset without using values, principles, or consequences.
13. Write a sentence template you can use to state a weak spot in the present tense.
14. Write a sentence template you can use to state damage as something a manager could notice.
15. What is the minimum information your chain must contain to be reviewable by someone else?

Acid Test practice

16. Give an example of an asset statement that would fail the Concrete Test.
17. Give an example of a weak spot statement that would fail the Current Test.
18. Give an example of a damage statement that would fail the Witness Test.
19. If only the Witness Test fails, what part are you allowed to rewrite?
20. Why is rewriting only the failing component important?

CIA classification

21. A damage statement says that an unauthorized person can view private records. Which CIA category is primary, and why?
22. A damage statement says that reports contain incorrect totals but the system is still running. Which CIA category is primary, and why?
23. A damage statement says that users cannot complete a required workflow during peak periods. Which CIA category is primary, and why?
24. What is one reason it can be misleading to list multiple CIA categories without choosing a primary one?

Friction thinking

25. Restate the friction rule in your own words.

26. What is one sign that a proposed change increases friction for authorized work too much?
27. What is one sign that a proposed change does not actually affect the weak spot?
28. Describe one change (in plain language) that tends to increase friction for unauthorized use while keeping authorized work close to the same.

Confidence check

29. Which component (Asset, Entry Point, Weak Spot, Damage) do you personally find hardest to make concrete, and why?
30. When you revise a chain, what is the one thing you check first to see whether the revision actually improved it?