# Chapter 1 Study Guide – Practical Core Software Security

## Chapter Overview

This chapter introduces the critical importance of software security, emphasizing the need to build security into the software development lifecycle (SDLC) via a Security Development Lifecycle (SDL). It outlines foundational concepts, such as the CIA triad, threat modeling, and the distinction between secure and quality code.

## Learning Objectives

* • Describe why software security is essential in modern systems.
* • Differentiate between software security and application security.
* • Distinguish quality code from secure code.
* • Explain the three core goals of SDL: Confidentiality, Integrity, and Availability (CIA).
* • Understand threat modeling and attack surface validation.

## Key Concepts & Definitions

### Software Security vs. Application Security

Software Security: Building secure software from the ground up using SDL within the SDLC.  
Application Security: Protecting the application after it's developed (e.g., with firewalls, WAFs).

### Quality vs. Secure Code

Quality Code: Reliable, maintainable, reusable.  
Secure Code: Resistant to exploitation, protects confidentiality/integrity.  
You need both — security is not an add-on to quality.

### The CIA Triad

Confidentiality: Preventing unauthorized access.  
Integrity: Preventing unauthorized modification.  
Availability: Ensuring systems are usable when needed.

### Threat Modeling

A process for identifying, ranking, and mitigating potential threats.  
Most effective before code is written.

### Cost of Fixing Defects

It is 50–200x more expensive to fix security flaws post-release than during early development.

## Important Quotes/Ideas

* • “Security must be built in from the very start.”
* • “Secure code is not necessarily quality code, and vice versa.”
* • “Threat modeling is the most time-consuming and misunderstood part of the SDL — but also the most critical.”

## Chapter Quick-Check (Practice Questions)

Q: What are the three goals of SDL?

A: Confidentiality, Integrity, Availability.

Q: Which activity is most effective when conducted before code development?

A: Threat modeling and attack surface analysis.

Q: Defective software is primarily a...

A: Software development and engineering problem.

Q: The cost to remediate flaws post-release can be how many times more expensive?

A: Up to 100 times.

## Exercises (Suggested Reflection/Research)

* • Visit the CSIS Significant Cyber Incidents site and consider how SDL practices could have prevented or reduced the impact of recent incidents.
* • Reflect: How does moving to the cloud or Agile development affect your organization’s SDL?
* • Pitch: How would you justify secure development training to your dev team or management?