Enterprise Security: Attacks and Defenses

Mohammad Saidur Rahman, Ph.D.

Department of Computer Science
The University of Texas at El Paso (UTEP)

https://www.rahmanmsaidur.com/

June 21, 2025

Lecture Overview

- Security Models
- Risk and Risk Analysis
  - How to define what you have and what's important
- Risk Management
  - what is it? Why is it "management" and not something else?
- Attacks
  - How can you assess risk w/out an understanding of possible attacks?
- Defenses
  - Once we define some attacks, begin to consider ways to defend

Quiz

15 MINUTES

https://tinyurl.com/quiz-mis-du

What We Learned So Far

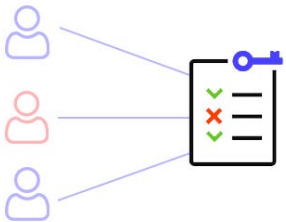
- **Security is Multi-faceted**: Covers network, system, cloud, AI, and physical domains.
- **Scaling Security**: From personal to enterprise-level risk and strategy evolve with scale.
- **Enterprise Security is Unique**: Strategic, budget-aware, people/process/tech driven.
- **Security is Not One Action**: It is a continuous, systemic process—no single fix.
- **Four Pillars of Security**: Computing systems, Networks, Cryptography, and Human behavior.
- **Policies & Organizational Dynamics**: Security policies, budgeting, and systemic risks play critical roles.
- **Ten Laws of Security**: From "Attackers always find a way" to "Security is a process."

Security Models

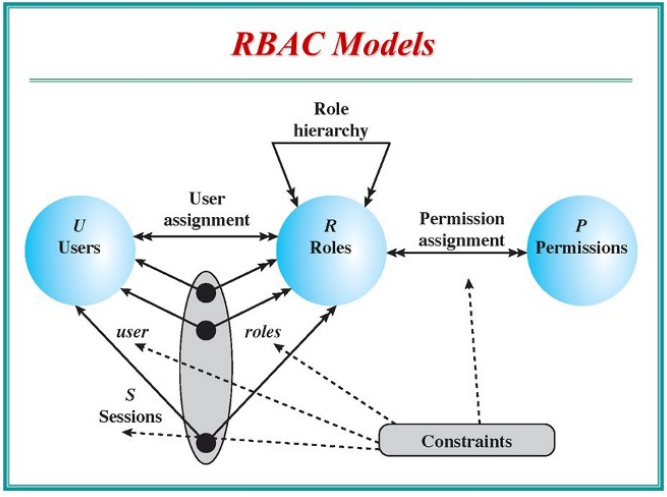
A computer security model is a framework for defining and enforcing security rules. It may be based on access rights, computation models, distributed systems, or no specific theory. These models are applied through security policies.

Example Security Model: ACL

Access Control List



Example Security Model: RBAC



Learn more! (google "security models"):-)

ACL v RBAC v ABAC[1] *v CBAC*[2] *v DAC*[3] *v MAC*[4] *v ...?*

[1] Attribute-Based Access Control
[2] Context-Based Access Control
[3] Discretionary Access Control
[4] Mandatory Access Control

How likely you are going to be attacked?

Attack Trees

Conceptual diagrams showing how an asset or target might be attacked.

The **GOAL** in this image is to open the safe.

The **PATHS** below show ways to perform the action.

Each of the blocks also has a letter (**I** or **P**) to indicate whether the method is likely based on current conditions.

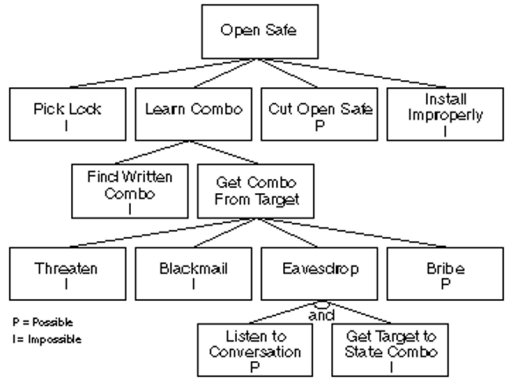


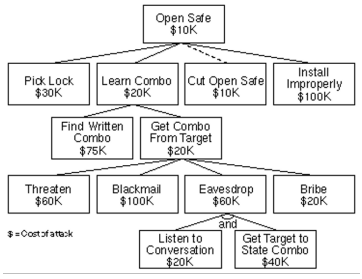
Image source: Bruce Schneier – schneier.com

How likely you are going to be attacked?

Attack Trees

The **GOAL** in this image remains to open the safe. If one has **KNOWLEDGE** about an attacker, the paths might include **COST** and need for **SPECIAL EQUIPMENT (SE)**.

IDEA: Find paths at lowest cost that require no special equipment — these are most likely to be exploited by an attacker. Protect those assets first! (Harder ones are less likely to be targets.)



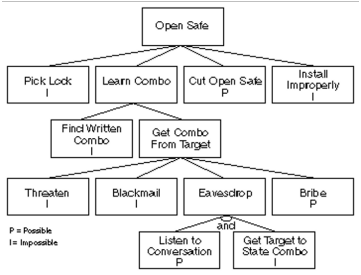


Image source: Bruce Schneier – https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Cyber Kill Chain (CKC)

Security Strategy has focused in the past on keeping the bad guys out.
Assumption: *if you keep out the bad guys you'll be safe.*

What's wrong w/this assumption?

Are you prepared to protect?

Understanding the Cyber Kill Chain

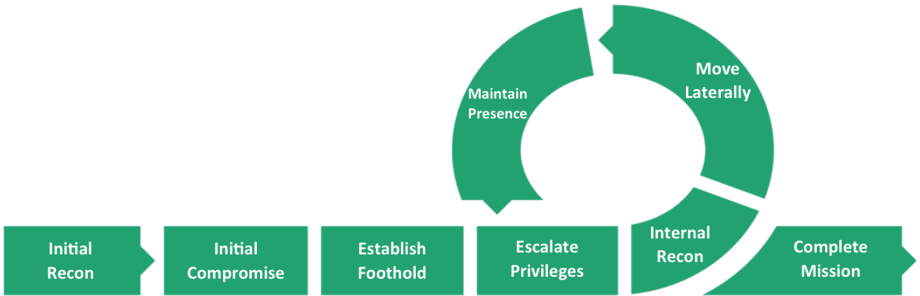
- Proposed by Lockheed Martin in 2011[5].
- The **end goal** is: *Complete the mission*.
- Each preceding step represents a stage attackers use to get closer to that goal.
- If you assume your network is **already breached**, adversaries may be found at **any stage** — not just at initial entry.

The Cyber Kill Chain is a series of steps that trace the stages of a cyberattack—from early reconnaissance to data exfiltration. It helps defenders understand and combat threats like ransomware, security breaches, and advanced persistent threats (APTs).

[5] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Are you prepared to protect?

Cyber Kill Chain



Risk Analysis

Key Questions and Considerations

- You can't protect everything — so how do you identify what's **most important**?
- Evaluate your organization: take inventory and define what is truly valuable.
- Define metrics to guide the assignment of appropriate security controls.
- If possible, understand the adversary:
  - Why do they want access?
  - How might they attempt to obtain it?
- Decide how to allocate your limited resources to maximize protection of critical assets.
- There is no one-size-fits-all solution — **every organization is different**.

Issues to Consider

- **Scale:** How does your risk model change as the organization grows?
- **Preventative Controls:**
  - How do you select the right tools, controls, and systems?
  - Many vendors compete—how do you choose wisely?
- **Detection:**
  - How do you detect if your prevention has failed?
  - Can you identify threats already inside your systems?

Issues to Consider

Assets

- Use NIST's *potential impact of loss* as a guide.
- How would you function without asset "X"?
- Assign higher scores to more valuable or mission-critical assets.

What is Risk Management?

Risk Management is a Process

- Analyze where compromises might occur.
- Define the consequences of those compromises.
- Identify ways to reduce the **probability** and/or **severity** of compromise.
- If you can fully prevent an incident — great!
- If not, plan for how to **limit the damage** and recover quickly.

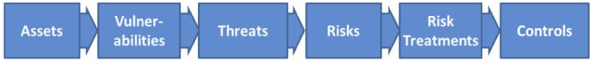
Risk Management Process

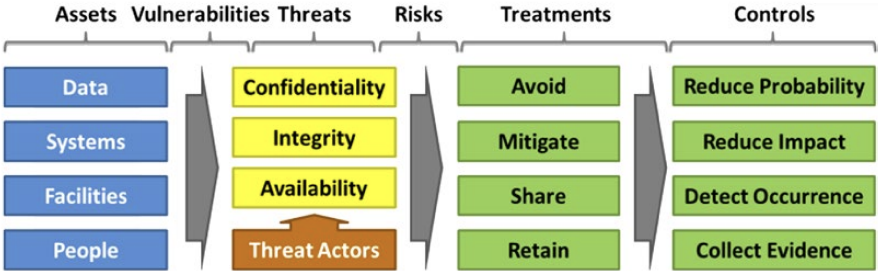
Addresses SIX areas and covers affected elements for those areas

Donaldson, Scott E., et al. "Managing an enterprise cybersecurity program." Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats (2015): 243-262.

Risk Management Process

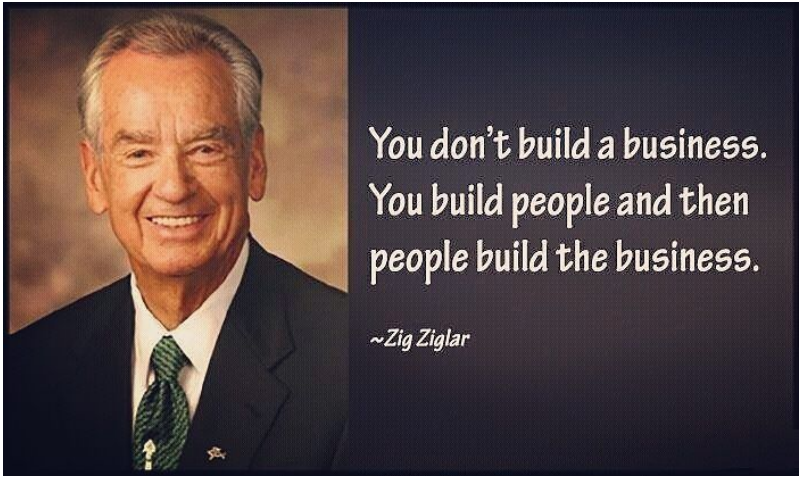
Addresses SIX areas and covers affected elements for those areas





Donaldson, Scott E., et al. "Managing an enterprise cybersecurity program." Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats (2015): 243-262.

Assets → People



Assets → Data

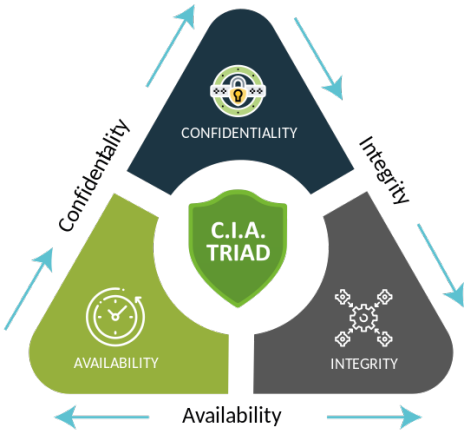
Assets → Systems

Assets → Facilities

Vulnerabilities, Threats, Attacks, Exploits

Vulnerabilities

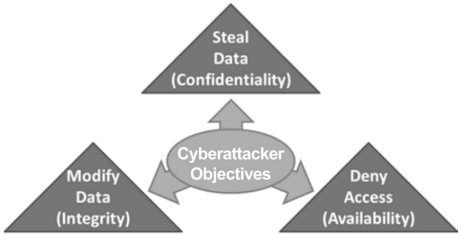
- A **vulnerability** is the quality or state of being exposed to the possibility of being attacked or harmed.
- In cybersecurity, vulnerabilities are typically understood in the context of the **CIA triad**:
  - **Confidentiality**
  - **Integrity**
  - **Availability**



Threats

- How can vulnerabilities be exploited?
  - This might be intentional, accidental, random, natural, man-made
- Consider creative ways to apply "Murphy's Law" Threats

  "Anything that can go wrong, will go wrong"



Risks

- No Threat? No Risk!
- No Vulnerability? No Risk!
- Therefore: Threats + Vulnerability = Risk
- Risk exists only when both a threat and a vulnerability are present.
- Defining risk involves:
  - The value of the asset
  - The severity of the threat
  - The understanding of the vulnerability
- This is ultimately a **judgment call**.

Common Pitfalls

- **Underestimation:** Failing to understand actual threats or vulnerabilities.
- **Risk Blind Spots:** Ignoring certain threats or missing them entirely.

Controls

Security Controls

To reduce risk, apply **security controls** — measures designed to manage, mitigate, or respond to potential threats and vulnerabilities.

Possible Outcomes

Security controls can help in one or more of the following ways:

- **Reduce probability** of a threat exploiting a vulnerability.
- **Reduce impact** if an exploit occurs.
- **Detect** when a threat event is occurring.
- **Collect evidence** for post-incident analysis, investigation, or legal action.

Attacks

- Offline Attacks: e.g., *Stuxnet*
- Viruses, Trojans, and Worms: Classic malware types
- Persistence / Command & Control: e.g., *Cobalt Strike*
- Custom-Created Malware: Tailored for specific targets
- Polymorphic Code: Constantly mutating to evade detection
- Intelligent Analysis: Adaptive, environment-aware behavior
- Automated and Polymorphic Attacks: Fully self-modifying delivery
- Firmware and Supply Chain: Targeting hardware and embedded systems

Types of attackers

Intent versus Motive

- Opportunistic Attacks
- Resources – Money – All fields
- Organized Crime
  - Resources/Information – Money – retail, health, finance
- Espionage
  - Trade Secrets – Money – tech, health, finance, defense
- Nationstate
  - Resources/Secrets – Military – defense, core infrastructure
- Hacktivist
  - Secrets – Attention – defense, energy, large corp, police

Vulnerabilities, Threats, Attacks, Exploits

- **Vulnerability**
  An identified weakness of a controlled system in which necessary controls are not present or are no longer effective
- **A threat**
  An object, person, or other entity that represents a constant danger to an asset
- **Attack**
  A deliberate act that exploits a vulnerability to achieve the compromise of a controlled system
  - Accomplished by a threat agent that damages or steals an organization's information or physical assets
- **Exploit**
  A technique or mechanism used to compromise a system

Onion Model of Cyberdefense

- The **target** (e.g., customer data) lies at the center.
- Surrounding the target are multiple **layers of defense**:
  - Controls (e.g., firewalls, authentication)
  - Monitoring mechanisms (e.g., IDS, SIEM)
- Each layer slows down or repels the attacker.
- The more layers in place, the harder it is to reach the target.
- Once inside the core, **all internal assets may be exposed**.

Garlic Model of Cyberdefense

- Targets remain at the **center**, but each is in its own isolated **enclave**.
- Each enclave is surrounded by its own **defensive layers** (controls, monitors).
- More layers = more difficulty for the attacker to reach the target.
- **Only the target within the breached enclave is exposed**; others remain protected.
- Requires an attacker to **independently breach each enclave**.

Implications

- **Takes more time to build** (architectural complexity).
- **Takes more time to breach** (higher attacker effort).

In-house and External Penetration Testing

- **Know your vulnerabilities** before attackers do.
- Be **ruthless and objective** — no room for internal bias or compromise.
- Build and test in your own **sandboxed environments**.
- Always maintain and validate a **disaster recovery plan**.

Question?