Introduction to Cybersecurity

Chang Phuong

Agenda

- What is Cybersecurity?

- Is Cybersecurity an Onion?

- What is CIA?

- What are the First 10 Principles (F10P) of Cybersecurity?

Learning Objectives

- Describe the purpose of Cyber Security

- Explain the multiple layers of Cyber Security

- Describe the principles of CIA

- Explain the concepts of First 10 Principles of Cybersecurity

What is Cybersecurity?
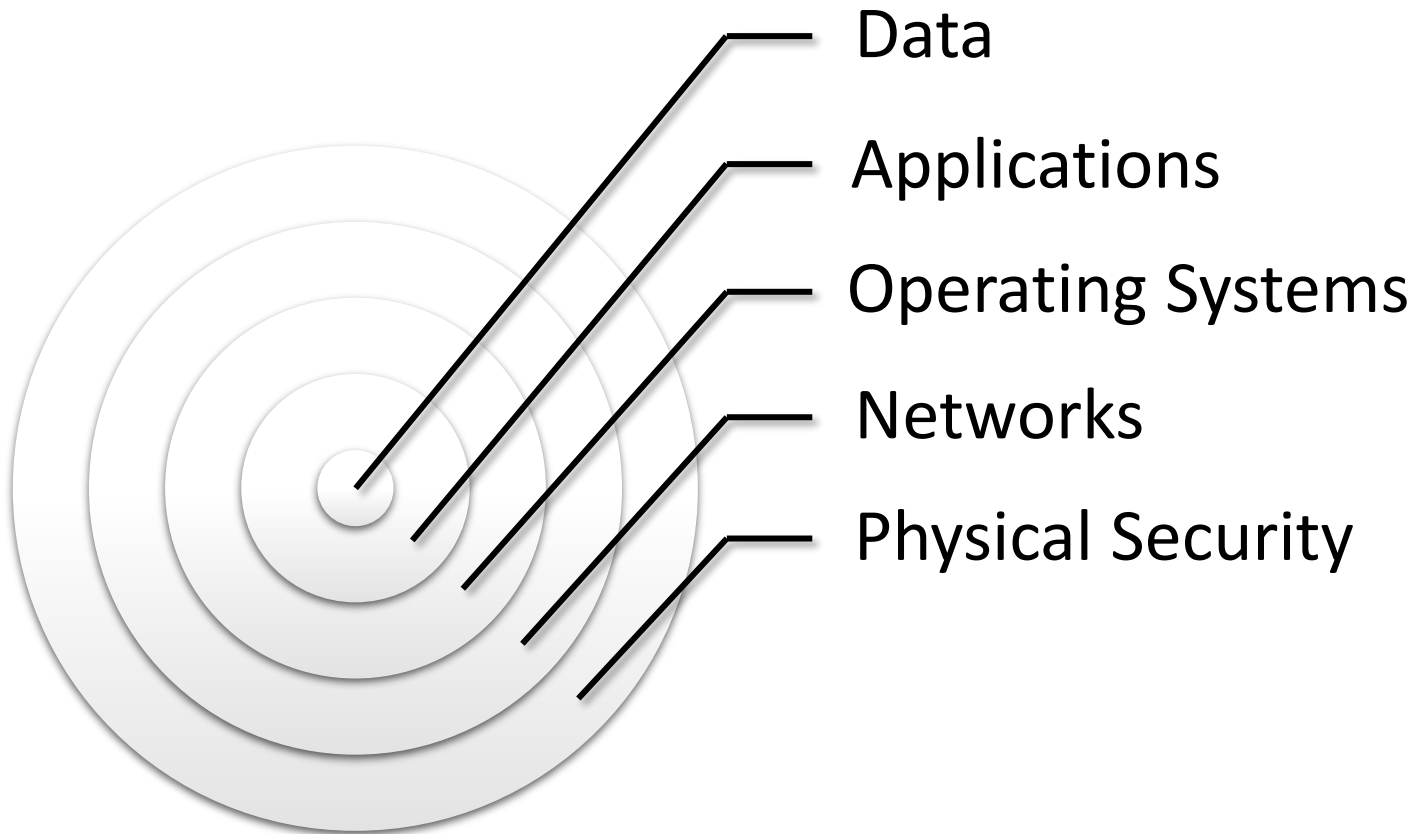
Why is Cybersecurity important?

Is Cybersecurity an Onion?

The Onion

- Data
- Applications
- Operating Systems
- Networks
- Physical Security

Detection Influencers

- **Risks** – potential loss/harm related to technical infrastructure, use of technology or reputation of an organization

- **Vulnerabilities** – a weakness which can be exploited by a threat actor to perform unauthorized actions within a computer system

- **Attacks** – SQL Injection, DNS Tunneling, MITM, DOS, Phishing

Vulnerabilities

Risks

Attacks

Security Onion
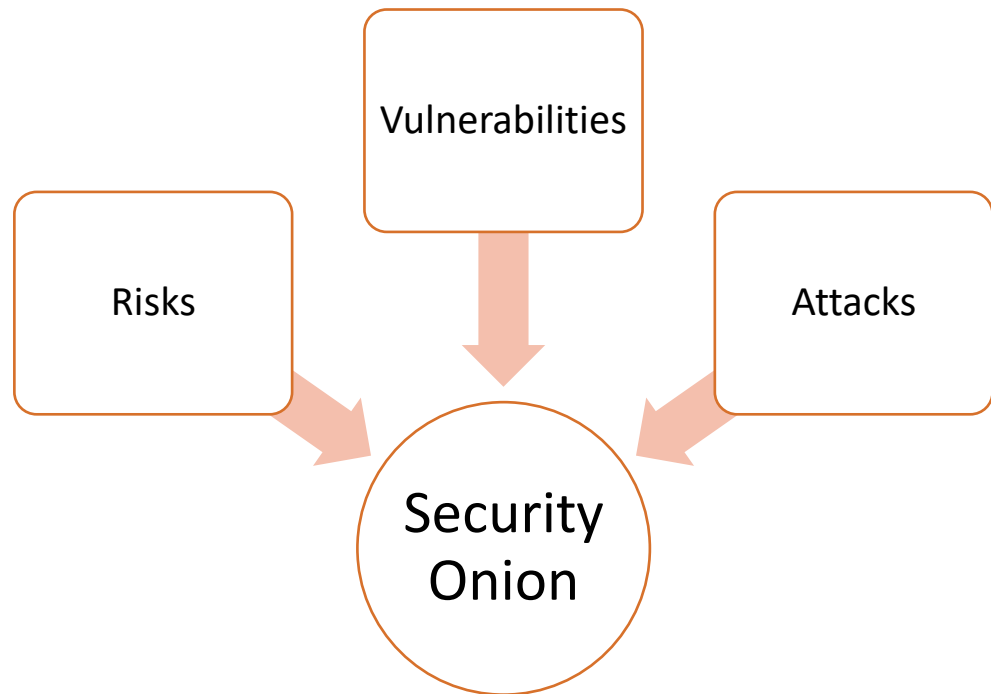
Prevention Influencers

- Regulations – directives that safeguard computer systems with the purpose of forcing companies and organizations to protect their systems and information from cyberattacks

- Policies – informs company users of their obligatory requirements for protecting the technology and information assets of the company

- Best Practices – NIST CSF, OWASP, ISO 27001, CSC, FAIR, etc

Policies

Regulations

Best Practices

Security Onion
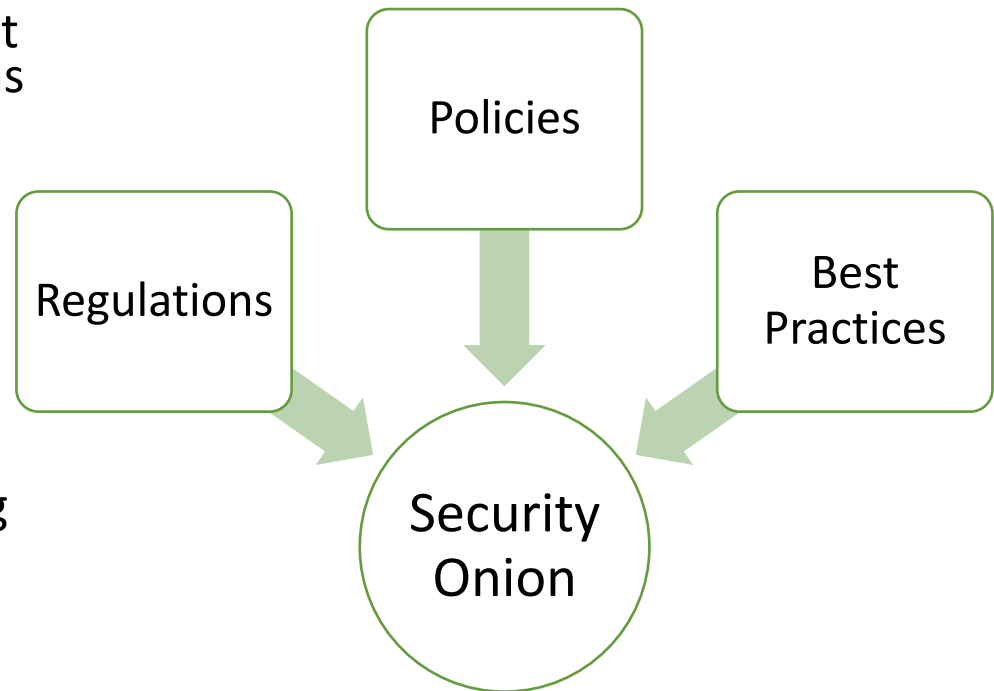
Cybersecurity CIA Triad
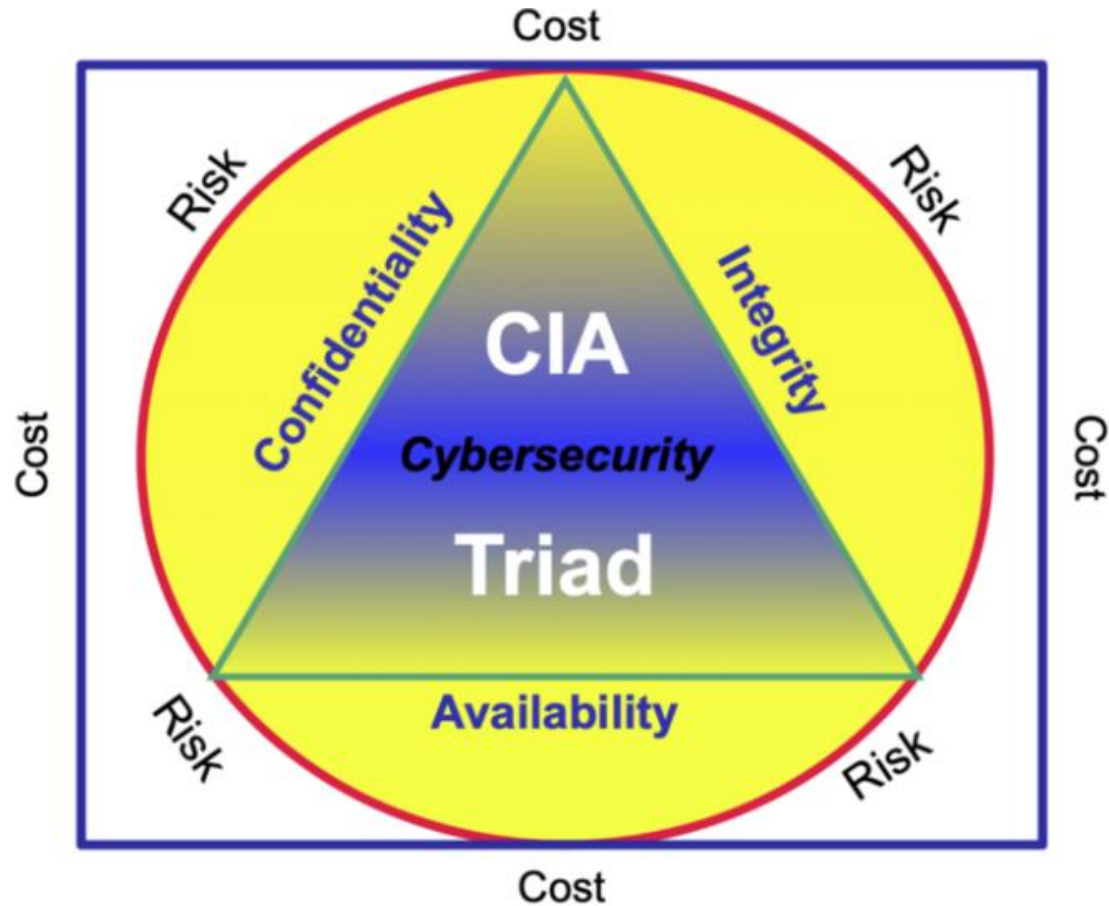
First 10 Principles of Cybersecurity

1. **Abstraction** – a general concept or idea, rather than something concrete or tangible, a simplified version of something technical

2. **Data Hiding** – providing information on a "need to know" basis

3. **Domain Separation** – clearly defined scope of ownership and responsibilities

4. **Layering** – functional components and activities that interact with each other

5. **Least Privilege** – minimum level of access needed to perform a job function

First 10 Principles of Cybersecurity

6. **Minimization** – reduce cost, complexity, and footprint

7. **Modularity** – breaking down complex concepts into manageable pieces for implementation and maintenance

8. **Process Isolation** – preventing a process from influencing or affecting another process without permission

9. **Resource Encapsulation** – granting access to data necessary to complete a job function

10. **Simplicity** – keep it simple

Activity

- See the Trashketball and First Ten Principles handout and complete the activity