Introduction to Cybersecurity

1G
CYBER

Security is protection. Protection from threat actors. Those who will harm, intentionally or otherwise.

WHAT IS CYBERSECURITY?

Cybersecurity refers to the body of technologies, processes, and practices designed to protect networks, devices, software, and data. These are protected from attack, damage, or unauthorized access.

Cybersecurity Models form the basis for each cybersecurity implementation.

- Organizations that use firewalls as the primary means of security are based

on a *perimeter security model*

- Organizations that implement a variety of security mechanisms are based upon a

layered defense model

Each cybersecurity design makes key assumptions:

1. What is fully trusted, partially trusted, and what is not trusted

2. Who has *access* to what valued *assets*

The model enables governance frameworks to serve as more effective and applicable guidance for protecting the computing environment. These are implemented as

Security Policy → Security Model → People, Process, Technology

Why do we need cybersecurity?

Components of information security:

- Computer Security
- Data Security
- Governance
- Management Systems
- Network Security
- Policy

The pillars of information security:

- Confidentiality
- Integrity
- Availability

Known as the C.I.A Triad

CYBERSECURITY GOVERNANCE

- The typical driver for cybersecurity governance remains the prevention of fraud and abuse
- Prevention of abuse and fraud have led to increased regulations, standards, and guidelines.
- Organizations now pay greater attention to governance, which has changed the dynamics of information security management.
- Computer crimes & cyber attacks are on the rise, many of which are perpetrated using social engineering techniques.
- Building security awareness into the governance structure has become essential.
- Information security professionals are faced with ever-evolving technologies. These include sophisticated and determined cybercriminals and a blended threat landscape.
- Even those security practitioners who work in non-regulated environments are expected to follow a common set of practices, criteria, and standards.
- An understanding of the laws, regulations, and standards that apply to the field of information security is essential.
- The most common frameworks are the National Institute of Standards and Technology (NIST) and International Organization for Standardization (ISO 27001 and ISO 27002).

CYBERSECURITY CONTROL FAMILIES (Based on ISO 27001)

- Access Control
- Awareness and Training
- Audit and Accountability
- Security Assessment and Authorization
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection
- Planning
- Personnel Security
- Risk Assessment
- System and Services Acquisition
- System and Communications Protection
- System and Information Integrity
- Program Management

KEY INFORMATION SECURITY CONCEPTS

- **Access –** A subject of objects ability to use, manipulate, modify, or affect another subject or object.
- **Asset** – The resources that are being protected - workstation, servers, and network devices.
- **Attack –** A intentional or unintentional act that can damage or compromise information systems.
- **Control, Safeguard, or Countermeasure –** The security mechanisms, policies, or procedures that counter attacks, reduce risk, and resolve vulnerabilities
- **Exploit –** A technique used to compromise a system.
- **Exposure –** A state of being exposed when a vulnerability exist.
- **Loss –** A instance of an information asset suffering damage.
- **Risk –** The probability of an unwanted experience such as a loss.
- **Subject and Object –** These people and assets in the IT infrastructure.
- **Threat –** The danger to an information asset.
- **Vulnerability –** A weakness or fault in a system or protection mechanism.

THE THREE DIMENTIONS OF THE CYBERSECURITY CUBE

Manage Protection

- Domains
- Internet
- Network

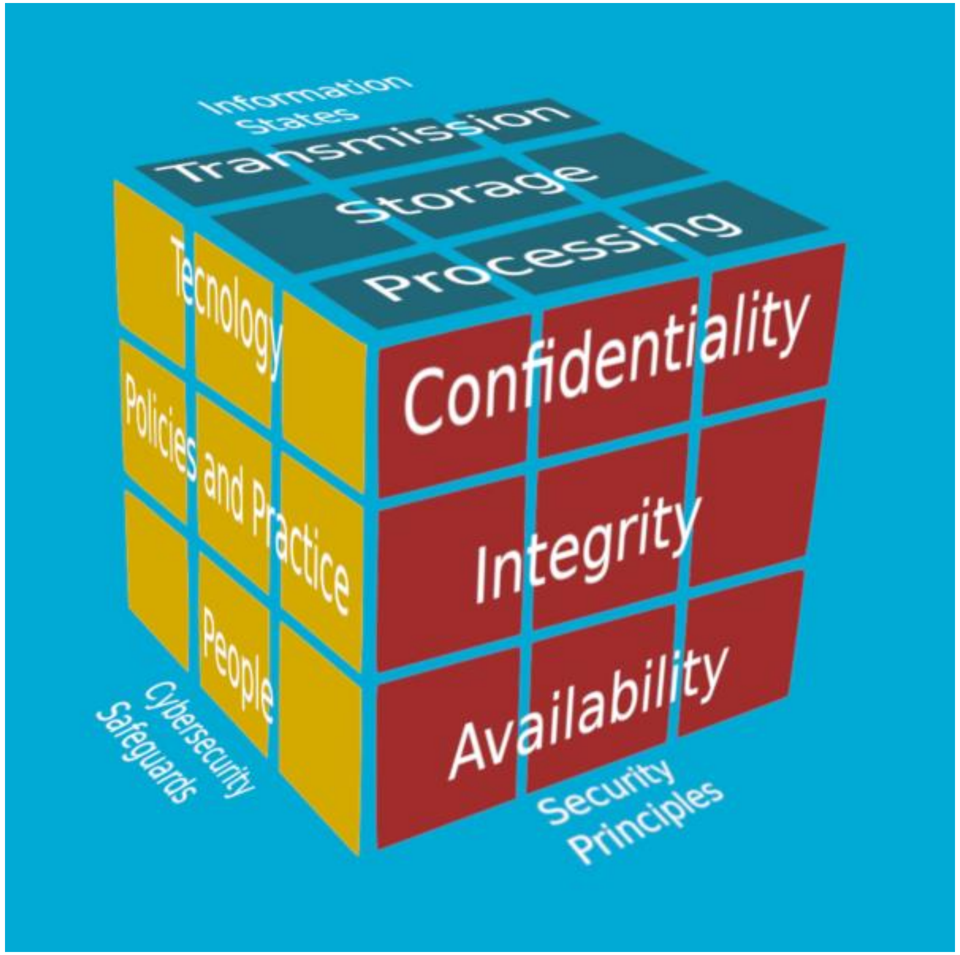
Three foundational principles:

- Information States
- Critical Information Characteristics
- Security Measures.

Information states include Transmission, storage, and processing.

Critical Information Characteristics include confidentiality, integrity, and availability.

Security Measures include technology, policies and practice, and the education, training, and awareness of people.

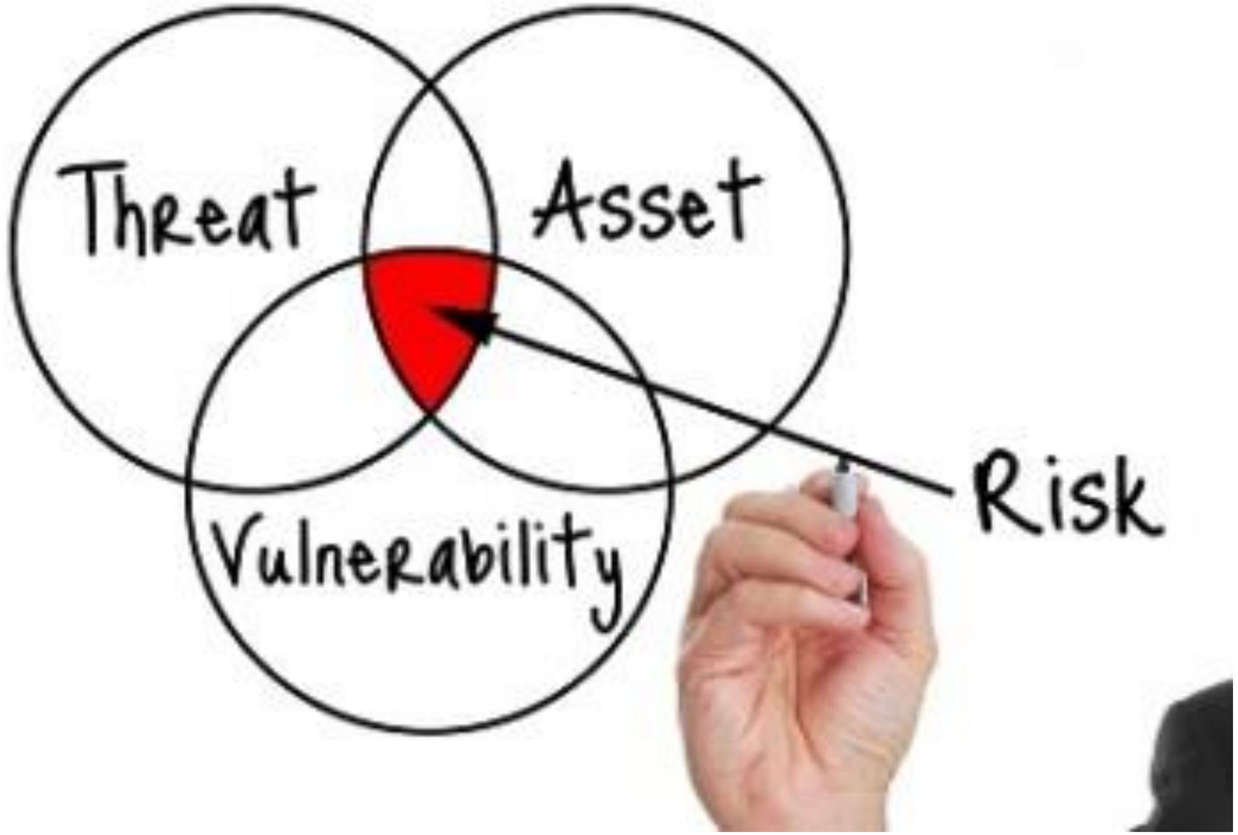


BALANCING INFORMATION SECURITY AND ACCESS

Manage Access

- Applications
- Data
- Encryption
- Network

The risk with people and information is balancing between access to information assets, threats, and vulnerabilities.

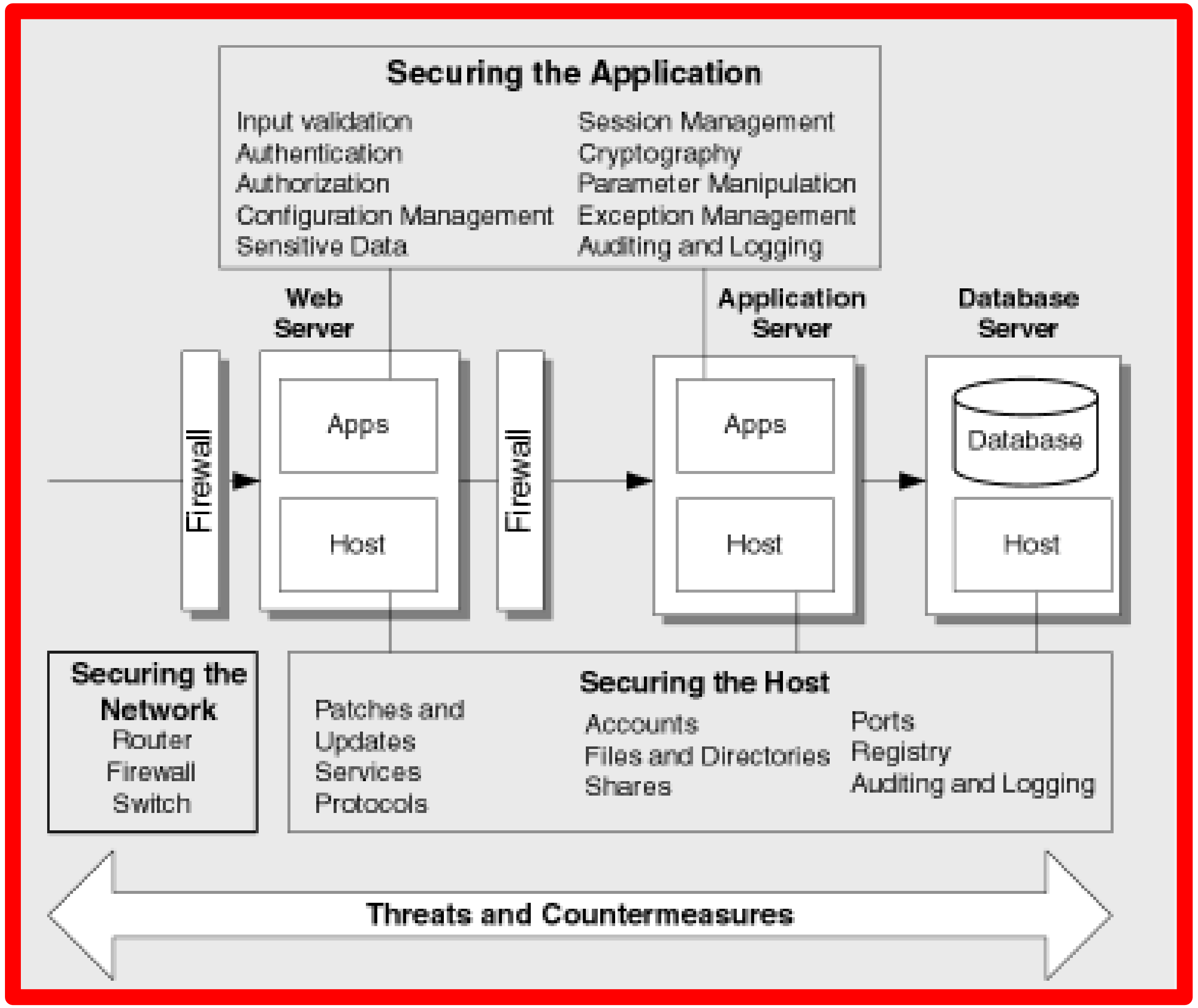


SECURITY PROFESSIONALS AND THE ORGANIZATION

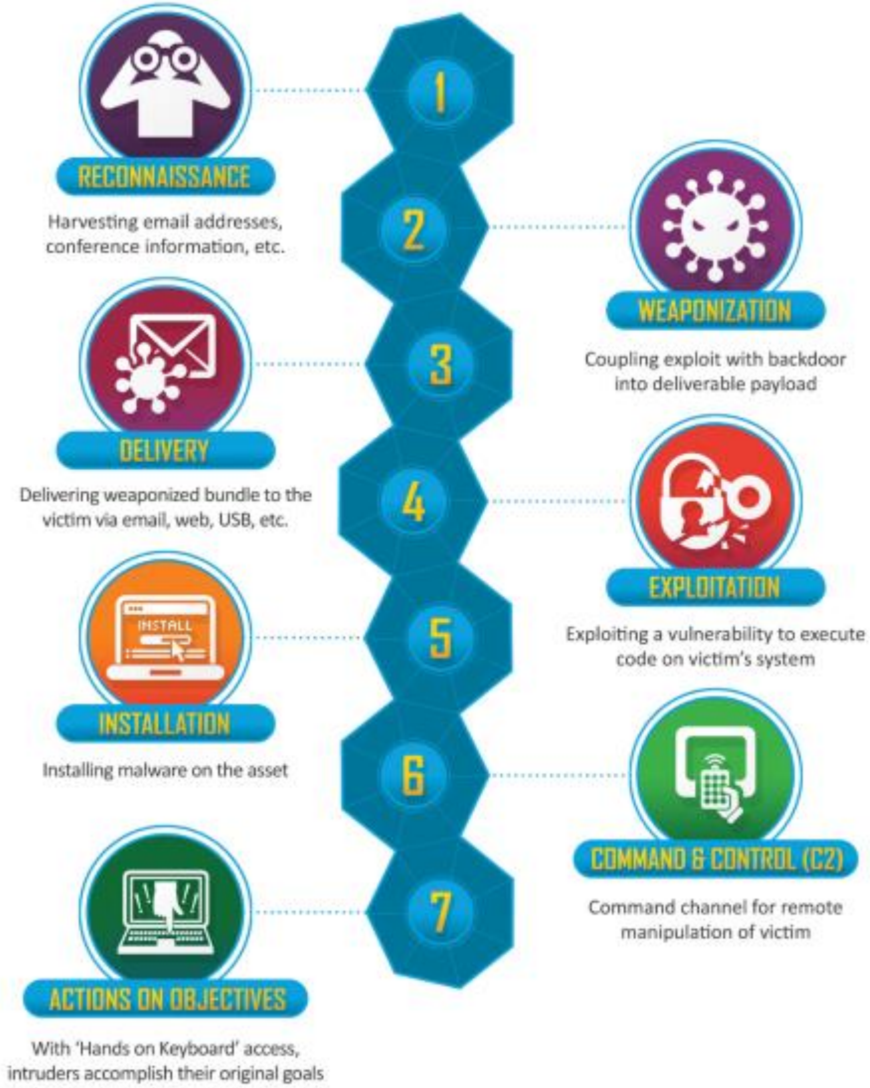
The Information Security Program

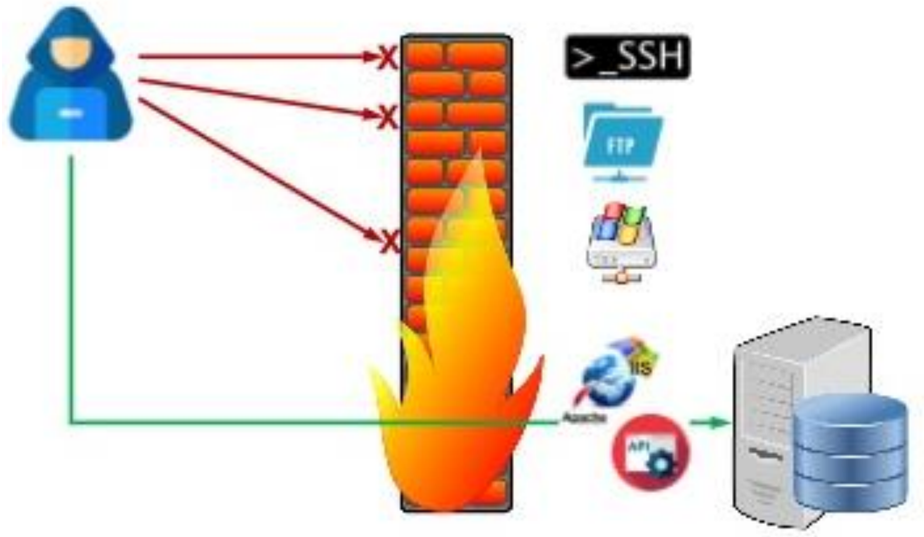
- Professional Training
- System Requirements
- System Design
- Implementation
- Verification
- Release
- Incident Response

Thinking about security helps to cut through the information overload. Incorporating cybersecurity frameworks, patterns, and best practices help to create a defense in-breath security paradigm. A skilled workforce helps to drive cybersecurity governance in the organization.



THE CYBERSECURITY KILL CHAIN


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

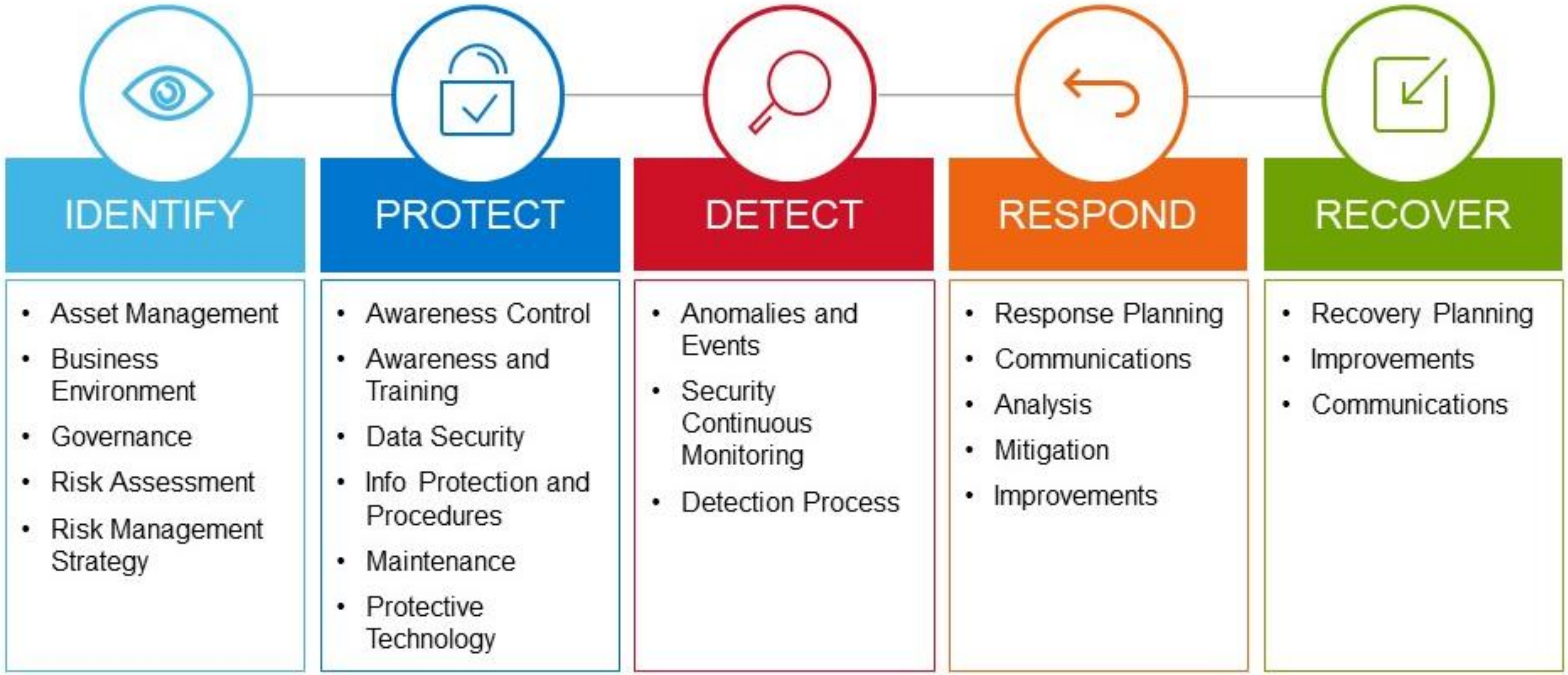


Stop The Threat

A framework that is part of the Intelligence Driven Defense model for identification and prevention of cyber intrusions. This model identifies what the threat actor must complete in order to achieve their objective.

The seven steps enhance visibility into an attack and enrich professionals with the understanding of an actor’s tactics, techniques, and procedures.

NIST CYBERSECURITY FRAMEWORK



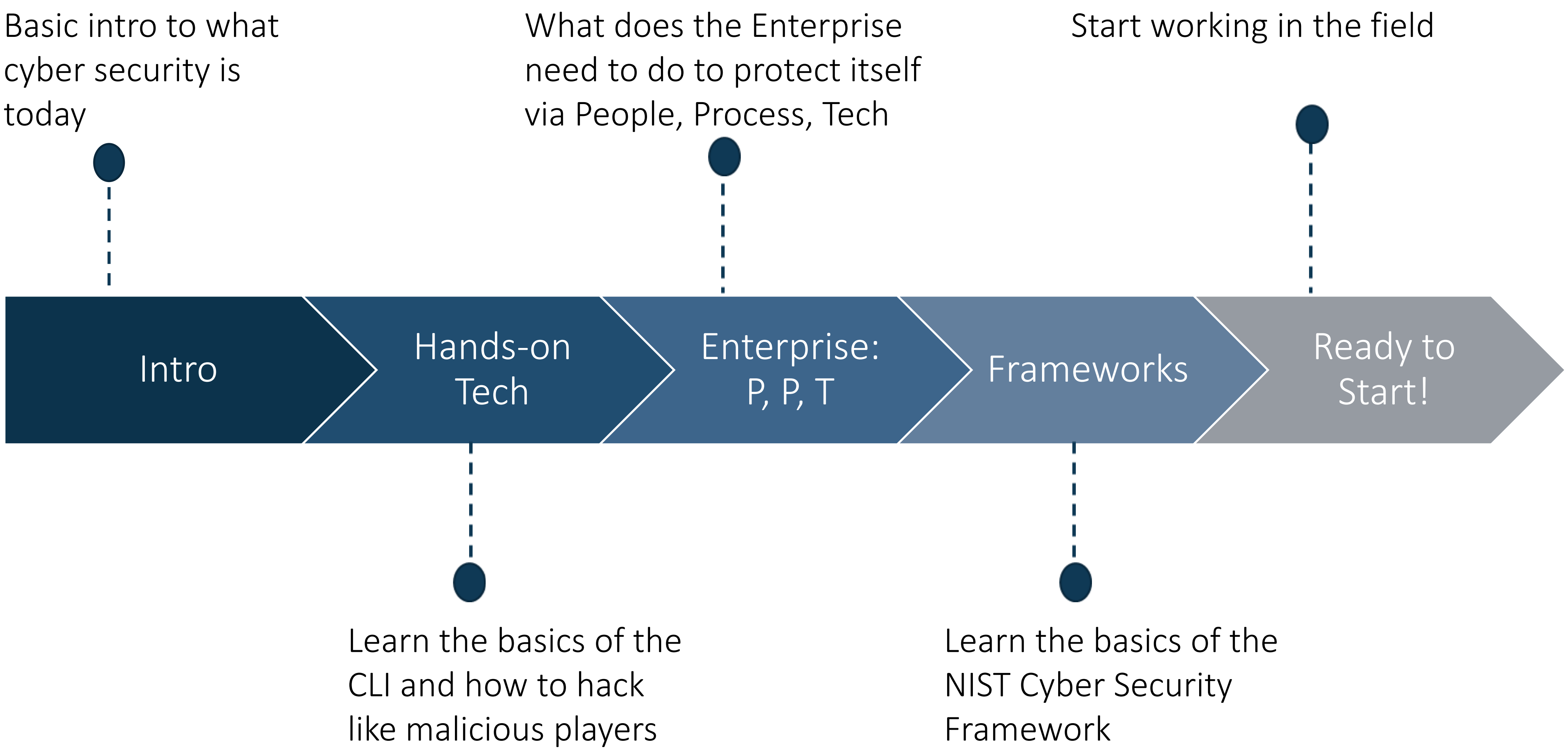
IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
• Asset Management • Business Environment • Governance • Risk Assessment • Risk Management Strategy	• Awareness Control • Awareness and Training • Data Security • Info Protection and Procedures • Maintenance • Protective Technology	• Anomalies and Events • Security Continuous Monitoring • Detection Process	• Response Planning • Communications • Analysis • Mitigation • Improvements	• Recovery Planning • Improvements • Communications

IMPLEMENTING STRATEGIC CYBERSECURITY GOVERNANCE

CRITICAL THINKING FOR SITUATIONAL & OPERATIONAL INTELLIGENCE

	Identify	Protect	Detect	Respond	Recover
Reconnaissance	X				
Weaponization					
Delivery					
Exploitation					
Installation					
Command & Control					
Actions on Objectives					
	Deny	Degrade	Disrupt	Deceive	Destroy

PUTTING IT ALL TOGETHER



Basic intro to what cyber security is today

What does the Enterprise need to do to protect itself via People, Process, Tech

Start working in the field

Learn the basics of the CLI and how to hack like malicious players

Learn the basics of the NIST Cyber Security Framework

THANK YOU

1G CYBER