**Cyber Security Essential**

**Script kiddies:** The use built in tools and scripts to harm the organization.

**Vulnerability Broker**: The attempt to find vulnerabilities and report to vendors for prize and rewards.

**Hacktivists:** They protest against any organization and government by leaking videos, sensitive information’s basically the are gray hat hackers.

**Measures to thwarting Cybercriminals:**

**Vulnerability Database:** The Common vulnerability and exposure (CVE) database was develop to publicly available of all known vulnerability.

**Early warning system:** Early system warning system display the Realtime visualization of map road of attack

**Sharing cyber intelligence:** InfraGard is an example of sharing cyber security intelligence. InfraGard is partnership between FBI and private sector. The purpose of sharing this information is to prevent from cyber-attacks.

**ISM Standards:** The ISO/IEC 2700 are the standards to measure the management of security with in organization.

**New Law:** These ISACA law can address to protect the intellectual property of person.

**2: The National Cybersecurity Workforce Framework**

It will be divided into 7 categories.

**Operate and Maintain:** This specialty area is responsible for providing support and maintenance. The also ensure the performance and security of an information security system.

**Protection and Defend:** This specialty area is responsible for identification, analysis and mitigation of threats to internal information technology system or network.

**Investigate:** This specialty area is responsible for investigation for cybercrime/event occurred in system/organization.

**Collect and operate:** this specialty area responsible for collection of cybersecurity information that may be used to develop intelligence to protect next time.

Analyze: This Specialty area is responsible for highly specialized review and evaluation of incoming cybersecurity information to determine it is usefulness for intelligence.

**Oversight and Development:** this specialty area is responsible for providing leadership, management, direction or development and advocacy. So that individual and organization may effective conduct cybersecurity work.

**Securely provision:** This specialty area is responsible for conceptualizing, designing and building

Secure information technology system. e.g.: responsible for some aspect of system development.

**The Principle of security:**

**Cybersecurity Cube:**

**1: Security Principle:**

**Confidentiality:** Restrict the unauthorized person from information resources or processes.

**Integrity:** refer to the accuracy, consistency and trustworthiness of data.

**Availability:** It ensure information is available when we needed.

**2: Information State:**

Data has three possible state:

1: Data in transit.

2: Data in storage.

3: Data in process.

**3: Counter Measures**

1: policies and practices.

2: Technology.

3: People.