Cyber Security Tools and Technologies

Dr. Arshad Ali
Associate Professor
NUCES Lahore

Acknowledgment

Google Cyber Security Learning Module Assets, Threats and Vulnerabilities

Security Guidelines

- ✓ Organizations mostly face an overwhelming amount of **risk.**
- ✓ Developing a **security plan** from the beginning that **addresses all risk** can be challenging.

- ✓ This makes **security frameworks** a useful option.
  - ✓ For example: **NIST CyberSecurity Framework (CSF)**
    - ✓ Being flexible and a voluntary framework can be applied to any industry.

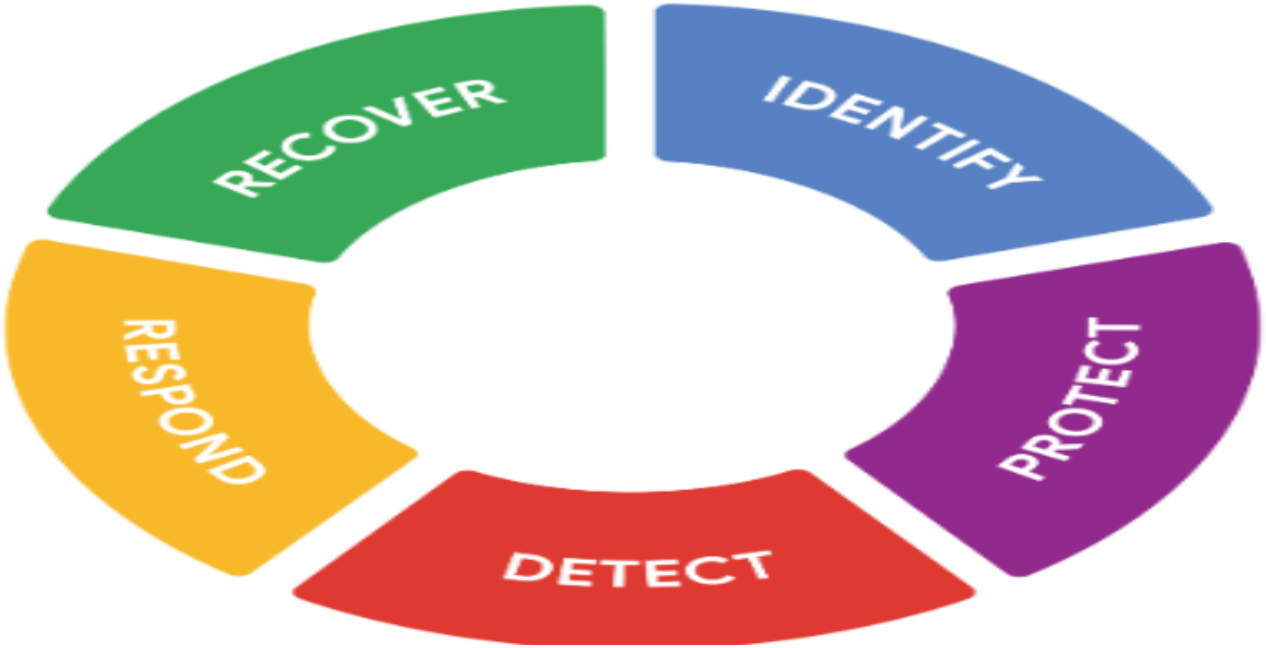
CSF Origins

- NIST developed CSF to **protect critical infrastructure** in the United States.
  - Because NIST was an unbiased source of scientific data and practices.
- NIST eventually **adapted** the CSF to fit the needs of businesses in the public and private sector.
- **Goal:** to make the framework more flexible,
  - making it easier to adopt for small businesses or anyone else
  - that might lack the resources to develop their own security plans.

CSF Components

NIST CSF consists of 3 components

- core, tiers, and profiles
- **CSF Core** is a set of desired cybersecurity outcomes that help organizations customize their security plan.
- It consists of five functions, or parts



CSF Components

- **CSF Core** functions are commonly used as an **informative reference** to help organizations
- ***identify*** their most important **assets**,
- ***protect*** those **assets** with appropriate safeguards.
- understand ways to ***detect* attacks,** and
- **develop *response*** and ***recovery* plans -** should an attack happen.

CSF Components

- **CSF Tier** are a way of measuring an organization's cybersecurity program.
- CSF tiers are measured on a scale of 1 to 4.
- **Tier 1 is the lowest score**, indicating that a limited set of security controls have been implemented.
- Overall, CSF tiers are used to assess an organization's security posture and identify areas for improvement.

CSF Components

- **CSF profiles** are pre-made templates of the NIST CSF that are developed by a team of industry experts.

- CSF profiles are tailored to address the specific risks of an organization or industry.

- They are used to help organizations
  - develop a baseline for their cybersecurity plans, or
  - as a way of comparing their current cybersecurity posture to a specific industry standard.

CSF Components

- The core, tiers, and profiles were each designed to help any business improve their security operations.

- Although there are only three components, the entire CSF framework consists of a complex system of **subcategories and processes**.

Implementing CSF

Compliance – an important concept in security

- **Compliance** is the process of **adhering to internal standards and external regulations**.
- Compliance is a **way of measuring** how well an organization is **protecting their assets**.

- CSF consists of **standards, guidelines, and best practices** to manage cybersecurity risk.
- Organizations may choose to use the CSF to achieve compliance with a variety of regulations.

Regulations are rules that *must* be followed, while **frameworks** are resources you can *choose* to use.

Implementing CSF

- Though many businesses have used the NIST CSF since it was created.
  - However, its implementation can be a challenge to due to its **high level of detail**.
- It can also be difficult to find where the framework fits in. E.g.,
  - some businesses have established security plans, making it unclear how CSF can benefit them.
  - some businesses might be in the early stages of building their plans and need a place to start.

Implementing CSF

- U.S. Cybersecurity and Infrastructure Security Agency (CISA) provides detailed guidance that any organization can use to implement the CSF in any scenario.

Summary of CISA recommendations:

- **Create a current profile** of the security operations and outline the specific needs of your business.
- **Perform a risk assessment** to identify which of your current operations are meeting business and regulatory standards.
- **Analyze and prioritize existing gaps** in security operations that place the businesses assets at risk.
- **Implement a plan of action** to achieve your organization's goals and objectives.

Note: Always consider current risk, threat, and vulnerability trends when using the NIST CSF.