

Cyber/Analytical presentation

By Darren J, Paul C and Lorna V

CIA Triad

An **important** model that is used in information security that represents the the core **principles** of **Cyber Security**



Confidentiality

- **Assures the secrecy of a user data**

- **Assures that only the user that owns that data can access the data**

BREACH OF
CONFIDENTIALITY



Integrity

- Maintains the **accuracy** of the **data**
- **Prevents** the data from being **altered** but anyone who does **not** have **permission**

*Truth &
Integrity First
Honesty*

Availability

- **Guarantees** that data is **accessible** at **anytime**
- Assures that **data** can only be **accessed** by the **owner** of that data



Why is this important?



Examples

- ATM's
- File permissions
- Online shopping accounts



The NIST Cybersecurity Framework

It's a U.S. federal agency that develops **technology, standards, and guidelines** to promote innovation and improve the quality of life—especially around **measurement science, engineering, and cybersecurity**. ([nist.gov](https://www.nist.gov))

What does it Do?



1. Develops Standards and Guidelines

Creates technical standards used in industries ranging from manufacturing to cybersecurity

2. Cybersecurity Leadership

Go-to authority for cybersecurity best practices.

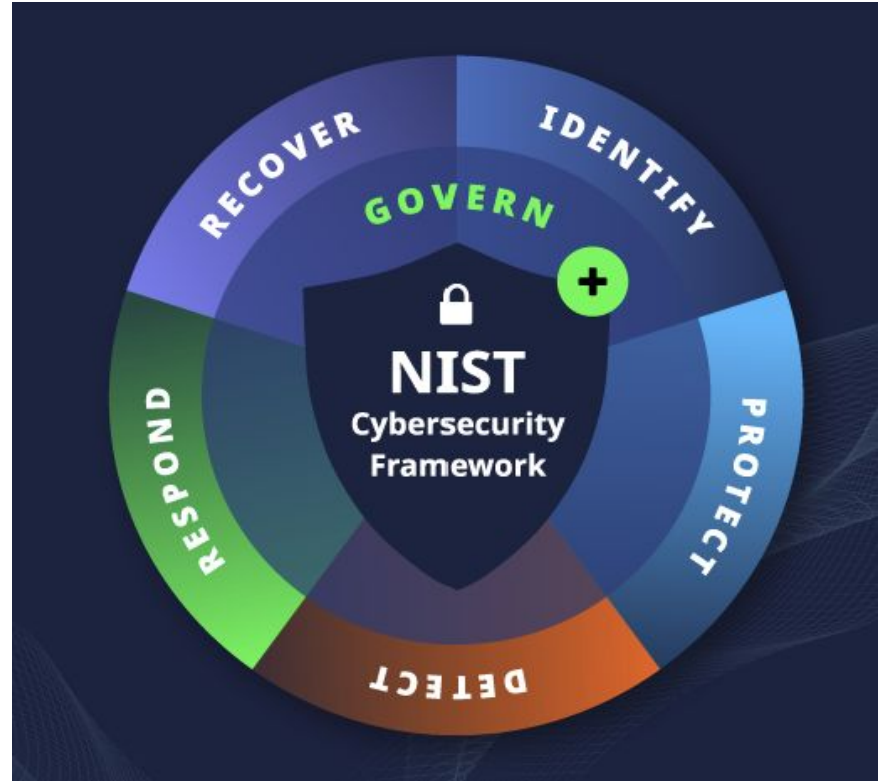
Identify, manage, and reduce cybersecurity risks.

3. Supports Innovation and Commerce

Provides standards and measurements that businesses rely on

6 Core Functions of the NIST Cybersecurity Framework (CSF 2.0)

1. **Govern** 🏛️
2. **Identify** 🔍
3. **Protect** 🛡️
4. **Detect** 🚨
5. **Respond** 🧯
6. **Recover** ♻️



Why It Is Important?

-  1. **Standardized Yet Flexible**
-  2. **Improves Risk Management**
-  3. **Regulatory and Industry Recognition**
-  4. **Boosts Stakeholder Confidence**

Real-world Impact

- 1. **Practical**
- 2. **Widely Recognized**
- 3. **Continuously Updated**

Critical Infrastructure

- **Critical Infrastructure refers to essential systems we need for daily life.**

- **Examples include:**

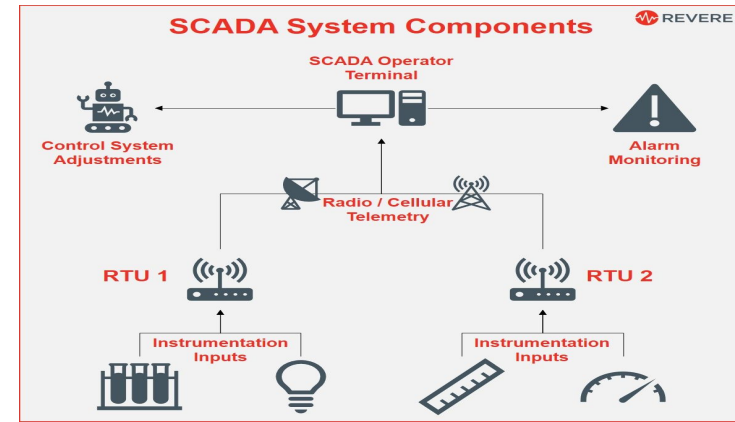
- **Electricity**
- **Water**
- **Transportation**
- **Communications**
- **Schools**
- **Hospitals**
- **Agriculture**



- Critical Infrastructure is largely dependant upon information technology and digital systems
- We use SCADA to control most critical infrastructure

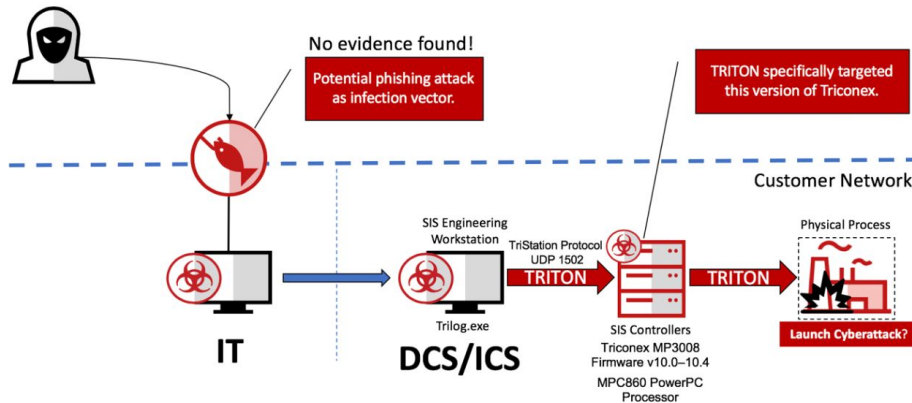
(Supervisory Control and Data Acquisition) SCADA Systems

- **What are SCADA Systems**
 - SCADA Systems are a control panel that can monitor and control industrial processes
- **Why are SCADA Systems Important**
 - SCADA ensures the efficiency, safety, and uptime of Critical Infrastructure



Security Risks of SCADA

- Security Risks
 - **Legacy systems and devices**
 - Critical infrastructure systems are outdated and still use default settings, making them vulnerable.
 - **Lackluster policies and procedures**
 - Weak policies lead to poor security practices, like no updates or weak passwords. Which creates many vulnerabilities.
 - **Lack of network segmentation**
 - Enables network breaches and lateral movement



How to Secure Critical Infrastructure

- Techniques
 - Implement **efficient and effective policies and procedures**
 - Implement a security focused environment
 - Require MFA
 - Strong password practice
 - Proper access controls
 - **Keep systems up-to-date**
 - Regularly update and replace equipment
 - **Increase network security**
 - Create a secure network by implementing network audits
 - IDS (Intrusion Detection Systems)
 - Firewalls
 - proper network segmentation





Common Cyber Threats

CYBER 
SECURITY

What are common cyber threats

- Common cyber threats are threats to the **security** of a **users data** that can happen **often**



Why is it important to know these threats

- Personal benefits
 - **Protection** from **simple** cyber attacks
 - Online **safety**
- Company benefits
 - **Protecting** customers information
 - Build **trust** with customers



Phishing attacks

- Attackers send scam **emails**, **text messages** or **calls** that contain **malicious** information or links that aims to **steal** something from the victim



Extra examples

1. Advanced Persistent threats (**APT**)
2. **DDoS** attacks
3. **Insider** attacks
4. Malware
5. **Password** attacks



Conclusion

- **CIA Triad**
 - Confidentiality, Integrity and Accessibility
- **NIST Cybersecurity Framework**
 - Govern, Identify, Protect, detect, respond and recover
- **Scada and Critical Infrastructure**
 - Monitor and control critical infrastructure systems
- **Common Cyber Threats**
 - Simple cyber attacks that can happen often
- **The Evolution Of Technology**
 - There needs to be new rules created as new technologies are invented