Situational Awareness a New Way to Attack Cybersecurity Issues Rather Than Using a System Defense Approach

Situational Awareness

The United States Army Field Manual defines *"Situational Awareness"* as "Knowledge and understanding of the current situation which promotes timely, relevant and accurate assessment of friendly, enemy and other operations within the battle space in order to facilitate decision making."

What does *"Situational Awareness"* mean to utilities cybersecurity and critical infrastructure and key resources (CIKR)?

The answer is

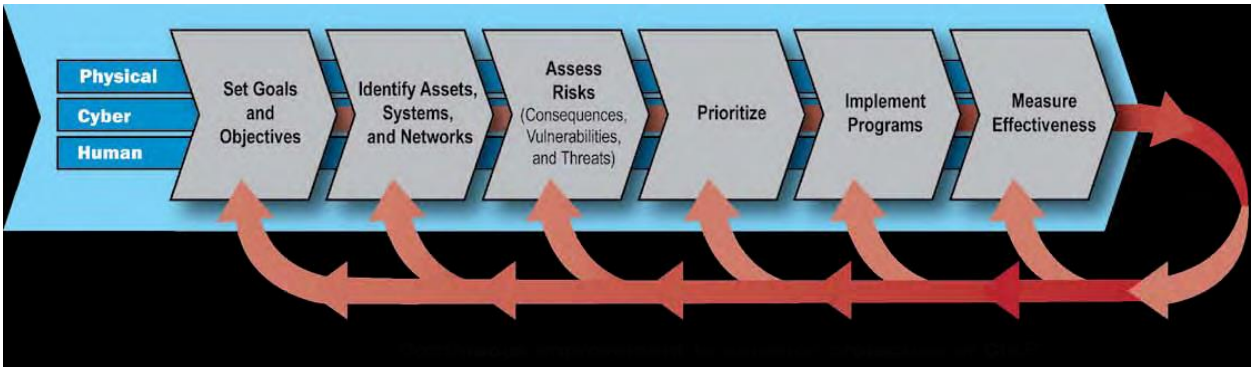
1) Accurate awareness of a utilities cybersecurity network and the CIKR that is a part of that network.
2) Complete understanding of the utilities cybersecurity operations and the individual CIKR that contribute to the overall process of the utilities system.
3) Proper assessment of the current operations occurring within the utilities cybersecurity network and the ability to assess potential breakdowns, weak areas or vulnerabilities that can be exploited to maximum effect in crippling a utilities system.
4) Monitoring of unusual events or occurrences within the cybersecurity network.
5) Flexibility to approach possible threats and mitigate them before they can be successful.

Situational Awareness is important due the complexity of operation in the modern utility system. However, in the case of cybersecurity the fluidity of change that occurs within the cybersecurity network evolves along an exponential rate that far outpaces other areas of a utilities grid. It is therefore essential that a utility and the industry have a unified approach to Cybersecurity and CIKR.

Unified Cybersecurity Process

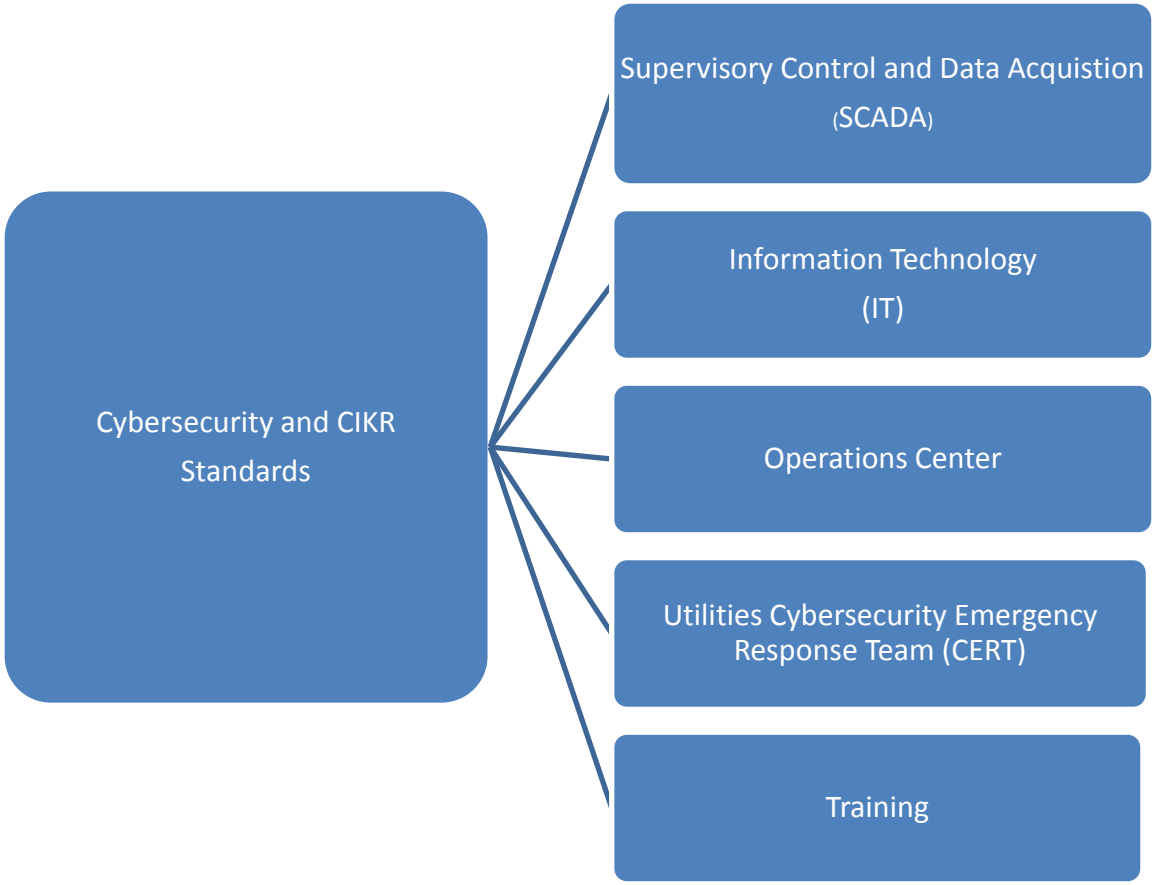
Under the current CIP Reliability Standards each utility has an approach to cybersecurity that is based on the Requirements in the CIP Reliability Standards. This current approach relies on the interpretation of the process to be used. While each system is unique in its operations the industry needs a unified process that is better defined and provides for a coordinated approach for utilities and regulatory agencies.

The Department of Homeland Security (DHS) National Infrastructure Protection Plan (NIPP) set forth a risk management framework that would provide the unified approach needed for a CIKR Risk Management Framework.



Cybersecurity and CIKR Framework

In developing a Cybersecurity and CIKR Standards we as and industry need to target the key components within the utility grid. This would constitute the following framework for standards.



Supervisory Control and Data Acquisition (SCADA) Standards

SCADA is the key component of the command and control of the transmission grid and transmission facilities structure. As a result of the importance of SCADA to grid operation, as a CIKR, standards need to be developed to address the security of the SCADA System. Some of the following considerations should be made within this section of a proposed standard.

1) Relay Equipment Access
    a) Password security
    b) Front Panel Buttons
    c) Front Panel Programming
    d) Relay Re-programming due to access by bypass of security or lack of security

2) Communication Hubs for SCADA such as RTU's and other communication devices, remote communication equipment (Microwave, Wireless and radio)
3) Physical Security of SCADA equipment
4) Guidelines on proper documentation of Cybersecurity inspections to include a process of observation of equipment compromise.
5) Guidelines for Cybersecurity Training for SCADA Technicians and Personnel.

Information Technology (IT)

Information Technology (IT) encompasses a vast area of technology within a utility that is continually evolving with a fluidity of change that exceeds the changes that happen within a power system. The areas that are affected by IT within a utilities power system are vast. Standards need to be developed that will provide a framework for IT Departments to provide security to each utilities system while providing them with the flexibility to address their networks unique conditions and to allow for the proper Situational Awareness within the utility.

Cybersecurity Emergency Response Team

For consistency Regional Transmission Organizations and individual utilities should have a Cybersecurity Emergency Response Team that would conduct itself as a fast acting unit in the matters of Cybersecurity and CIKR breaches and be able to identify potential Cybersecurity risks in order to allow mitigation of the identified weakness. Each utility, based on the uniqueness of their operations, should determine the type of personnel they want to assign to this unit, but it would be prudent that this unit be led by a qualified individual who understands the IT and Operation aspects of the utility. This team should be the central part of the utilities and RTO Cybersecurity program to provide continuity between the utilities, RTO's and the applicable Federal Agencies to include the DHS CERT.

Operations Center (OP Center)

The Operations Center provides the hub of all utility grid operation from the moment to moment operation of the transmission grid, the interconnection of generation on the system, the transfer of power between Balancing Authorities, the coordination of Market Participants offers and facilities and the coordination of power transfer between RTO's. The vast process managed by the OP Centers within the Nations Grid is critical point within the security and reliability of the National Grid. As a result standards should be developed to insure the security of the OP Centers and thereby secure the reliability of the National Grid. The standards should address the following issues.

1) Command and Control Centers
    a) The training and the appropriate documentation of training for OP Center Personnel
    b) Conducting a Preventative Maintenance Inspection (PMI) Program of the OP Center Facilities
    c) Emergency Plans
        i) Procedures for the loss of the OP Center and the Re-establishment of operations
        ii) Procedures for operation of OP Center under the condition of reduced staff due to Force Majeure or national security issues.
        iii) Procedure recommendations for Emergency Plan Exercises
    d) Security Plan and Procedure for different levels of access within the OP Center
        i) Security procedures when personnel no longer maintain employment status
        ii) Security procedures in the event of a security breach
    e) Implementation of a document process for OP Center day to day operations

Training

In all of the key areas of Cybersecurity proper training needs to be maintained and documented. Some Federal Training Requirements may need to become a requirement to fulfill certain areas of employment concerning Cybersecurity. Other Training should be the responsibility of the utilities and RTO's to meet the unique requirements of their systems. In all conditions there needs to be proper documentation to insure the qualifications of individuals operating in areas of Cybersecurity.