BENEFITS OF DEFINING AN ENTERPRISE SECURITY FRAMEWORK FOR ELECTRIC UTILITIES

There is a lot of activity in the electric utility industry today regarding the implementation of new information technology, cloud computing, server virtualization, mobile computing, smart grid, and effective disaster recovery processes. An underlying concern in moving forward with any of these initiatives is security.

Significant efforts have been made by most electric utilities to design and implement a security program that complies with the provisions of the NERC Critical Infrastructure Protection (CIP) Reliability Standards[1]. Additional requirements are on the drawing boards for new controls and methods for identifying assets and applying more stringent control requirements. Complicating this situation is the compliance requirements of SOX, HIPAA, PCI and other security standards as well as the need to manage risks in a wide variety of other informational systems, operational systems, and business processes.

From an enterprise security program perspective, in order to avoid redundancies and improve governance and efficiencies, the need for a common set of policies, procedures, and documentation provisions is a desirable objective, i.e., an integrated enterprise Security Program. A number of electric utilities have tried this approach which, unfortunately have many times resulted in an over cumbersome, ineffective and difficult to sustain and audit security program. The reasons for these failures have been associated with inadequate corporate governance, convoluted processes and procedures, and inadequate auditability provisions to name a few. In the meantime, addressing new technology opportunities is overwhelming from a security perspective.

There are considerable complexities present in establishing a common governance structure and security program to manage and sustain an enterprise-wide operation especially in a multifaceted environment such as the typical vertically integrated electric utility organization. As a designated Critical Infrastructure, electric utilities typically have a Bulk Electric System to operate, thousands of customers to support, multiple power generation facilities to operate and maintain, and hundreds of miles of transmission and distribution lines to manage via complex real-time systems. It is an extremely technology and data intensive operation.

It has been demonstrated that the development of an Enterprise Security Framework can serve as a foundation for establishing appropriate governance structures to facilitate the design, implementation, and operation of an integrated enterprise Security Program. A variety of think tank, education, and government organizations have developed a number of methodologies to establish an Enterprise Security Framework. The premise is that a determination needs to be made as to “what needs to be protected” in terms of the assets, systems, processes, people, and information for the entire enterprise.

A highly structured risk-based process has been established (through the requirements of the

[1] North American Electric Reliability Corporation (NERC) develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the Bulk-Power System through system awareness; and educates, trains and certifies industry personnel.

NERC CIP Reliability Standard) to identify "Critical Assets" specific to the operation of the Bulk Electric System. However, the need to identify the remaining assets, some of which are equally important to the utility, can become quite unmanageable without some structure and focus on the goal of the exercise. A similar risk-based approach will provide consistency in accomplishing this objective. A singular "asset/impact-oriented[2]" approach is appropriate to perform this analysis for electric utility organizations. The use of Critical Success Factors[3] (CSFs) to define areas of risks[4] for an organization is an effective and efficient approach to ensure risks are aligned with the mission, goals, and objectives of the organization. This holistic approach can effectively accommodate both regulatory compliance and meaningful security requirements for all operations of the enterprise.

The ultimate goal of course is to establish an enterprise-wide perspective that ensures a common Security Program is properly constructed, is not overreaching, constraining, or complex but meets the resiliency and security goals of the entire organization. Once the Enterprise Security Framework and underlying Security Program are established, assessing and implementing new regulatory requirements, technologies, and systems can proceed in an orderly manner.

Developing an Enterprise Security Framework will therefore provide:

- A governance structure that provides an enterprise view to manage and sustain an effective Security Program;
- Assurance that all relevant business and compliance risks are identified and aligned with the enterprise missions, goals, and objectives;
- A means to integrate multiple compliance requirements into a cohesive singular Security Program; and
- Identification of prioritized assets that need to be protected across the enterprise including informational and operational systems, physical assets, people, business processes, and information.

[2] As defined in NIST Publication 800-30, Guide for Conducting Risk Assessments. Revision 1, a risk assessment analysis approach can be: (i) "threat-oriented"; (ii) "asset/impact-oriented"; or (iii) "vulnerability-oriented". The "asset/impact oriented" approach is consistent with the NERC CIP Reliability Standard methodology and more appropriate for asset rich entities like electric utilities.

[3] Critical Success Factors defines key areas of performance that are essential for organizations to accomplish their mission". Reference Carnegie Mellon Software Engineering Institute Publication: The Critical Success Factor Method: Establishing a Foundation for Enterprise Security Management.

[4] Risk is defined as Probability of Occurrence times Impact.

For more information:

DYONYX, LP
solutions@dyonyx.com
1-855-749-6758